Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ingeniería de Sistemas e Informática

Unidad de Posgrado

Modelo de gestión de seguridad de la información para el E-Gobierno

TESIS

Para optar el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de la Tecnología de Información y Comunicaciones

AUTOR

Joel Enrique MERCADO ROJAS

ASESOR

Julio César ROJAS MEDINA

Lima, Perú

2016

Referencia bibliográfica

Mercado, J. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

692

13/R)
13

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMERICA
Facultad de Ingeniería de Sistemas e Informática
UNIDAD DE POSGRADO

SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAGÍSTER EN INGENIERÍA DE SISTEMAS E INFORMÁTICA
MENCIÓN EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

197

En la Ciudad Universitaria, a los Veintisiete (27) días del mes de mayo del 2016, siendo las 18:30 horas, se reunieron en el Aula Magna de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos, el Jurado Examinador de tesis conformado por los siguientes profesores:

Dra. Nora Bertha La Serna Palomino (Presidente).
Mg. Julio César Rojas Medina (Miembro Asesor).
Dra. Luz Sussy Bayona Oré (Miembro).
Mg. Ciro Aguilar Linares (Miembro).
Mg. Rómulo Fernando Lomparte Alvarado (Miembro).

Se inició la Sustentación de la tesis invitando al graduando ***Joel Enrique Mercado Rojas****, para que realizara la exposición oral y pública de la tesis para optar el Grado Académico de Magíster en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones, siendo la Tesis intitulada:*

"Modelo de Gestión de Seguridad de la Información para el E-Gobierno"

Concluida la exposición, los miembros del Jurado Examinador procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

18 DIECIOCHO MUY BUENO

Por tanto el Presidente del Jurado, de acuerdo al Reglamento de Grados y Títulos, le otorga al bachiller ***Joel Enrique Mercado Rojas*** *el Grado Académico de Magister en Ingeniería de Sistemas e Informática con mención en Gestión de Tecnología de Información y Comunicaciones, cuyo expediente debe ser remitido al Consejo de Facultad para su aprobación.*

Siendo las 19:30 *horas, el Presidente del Jurado Examinador da por concluido el acto académico de Sustentación de Tesis.*

DRA. NORA BERTHA LA SERNA PALOMINO
Presidente

MG. JULIO CÉSAR ROJAS MEDINA
Miembro Asesor

DRA. LUZ SUSSY BAYONA ORÉ
Miembro

MG. CIRO AGUILAR LINARES
Miembro

MG. RÓMULO FERNANDO LOMPARTE ALVARADO
Miembro

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO

"Tesis presentada a la Universidad Nacional Mayor de San Marcos, (Lima - Perú), para obtener el Grado de Magíster en Ingeniería de Sistemas, con la mención de Gestión de la Tecnología de Información y Comunicaciones".

Orientador: Mg. Julio Cesar Rojas Medina.

Universidad Nacional Mayor de San Marcos
Facultad de Ingeniería de Sistemas e Informática
Unidad de Postgrado

Lima – Perú
Mayo 2016

DEDICATORIA

Dedico este trabajo a mis padres y hermanos por animarme a seguir adelante. En especial a mis padres Avelino y Mercedes por el ejemplo de vida que me enseñaron y por la labor sacrificada hacia sus hijos en dar lo mejor y guiarnos en esta vida hacia el camino de la felicidad y el éxito.

AGRADECIMIENTOS

A Dios, por permitirme realizar mis estudios, en especial esta maestría en la Universidad decana de América, Universidad Nacional Mayor de San Marcos.

Al profesor y Asesor Mg. Julio Cesar Rojas Medina, por su orientación, dedicación y su alto grado de compromiso que ha sido un factor importante para que este trabajo de investigación cumpla con los objetivos trazados.

Al Mg. Rómulo Lomparte Alvarado, Mg. Percy Espino Menacho y Dr. Alberto Sotomayor Casas, por sus sugerencias brindadas y apoyo valioso en el presente trabajo.

A los profesores y personal administrativo de la Unidad de Postgrado del FISI de la UNMSM, por la calidad profesional y de servicio demostrado.

Al grupo humano de la Contraloría General de la República, por brindarme las facilidades para la realización del presente trabajo.

A mis hermanos Abel, Kathia, Roger y Llugomir, a mis grandes amigos Danny, Humberto, Javier y Roberto y a todas aquellas personas que de alguna y otra manera colaboraron con la realización de este trabajo de investigación.

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO

RESUMEN

Las entidades han reconocido el Gobierno Electrónico como una parte importante de acercamiento a los ciudadanos, mediante servicios automatizados basados en tecnologías de la información, más eficiente y con resultados significativos. Lo cual ha conllevado a enormes retos en seguridad de la información y serán aún mayores conforme vaya evolucionando a sistemas más complejos y sofisticados por el uso intensivo de internet.

En la actualidad las entidades del sector público no cuentan con un modelo de gestión de seguridad de la información para el Gobierno Electrónico que permita la implementación, supervisión y control de seguridad de la información de los procesos que brindan servicios automatizados basados en web.

En el presente trabajo se ha realizado la revisión de modelos de seguridad de la información, analizando su problemática, aspectos comunes y relevantes en la seguridad, por lo que se identificaron 08 elementos (fases, organización, funciones, documentos, niveles, controles, indicadores y métricas) que han permitido proponer un Modelo de Gestión de Seguridad de la Información para el Gobierno Electrónico.

La propuesta de modelo se orienta a los procesos que brindan servicios de gobierno electrónico, lo cual a través de una estructura organizacional y funciones permite implementar y gestionar la seguridad de la información de acuerdo a las fases establecidas y nivel de madurez requerido, mediante la actualización, mejora o desarrollo de documentos y controles; asimismo permite el monitoreo del nivel de seguridad a través de la revisión de los indicadores y métricas establecidas.

Palabras Clave: Gobierno electrónico y Seguridad de la información (SI)

INFORMATION SECURITY MANAGEMENT MODEL FOR E-GOVERMENT

ABSTRACT

The entities have recognized the E-Government as an important part of reaching citizens through automated services based on information technology, more efficient and with significant results. This has led to huge challenges in information security and will be even greater as it evolves to more complex and sophisticated systems for the intensive use of Internet.

At present public sector entities do not have a Information Security management Model for e-goverment to allow the implementation, supervision and control of information security of automated processes that provide web-based services.

In this work was carried out a review of information security models, analyzing their problems, common and relevant safety aspects, making 08 elements (phases, organization, functions, documents, standards, controls, indicators identified and metric) that they have allowed propose a management model Security Information for E-Government.

The proposed model is directed to processes that provide E-Government services, which through an organizational structure and functions allows the implementation and management of the information security according to the established phases and level of maturity required by updating, improvement or development of document and controls; It also allows monitoring of the security level through the revision of indicators and metrics established.

Keywords: E-Government and Information Security (IS)

INDICE GENERAL

LISTA DE CUADROS

LISTA DE FIGURAS

1. CAPITULO I: INTRODUCCIÓN

1.1. Situación Problemática

Durante las últimas décadas del siglo pasado diferentes avances técnicos produjeron grandes cambios en el mercado de la Tecnología de la Información (desde ahora "TI"), la cual ha girado en torno a los "datos"; su recopilación, almacenamiento, transmisión y presentación ha girado en torno a la "T" de la tecnología de información, cuando las nuevas revoluciones de la información giran en torno a la "I" de información [Drucker 1999].

Esta revolución de la información aportó gran parte de las oportunidades de desarrollo dentro del mercado global actual. Uno de los cambios de mayor disrupción fue el advenimiento de internet como tecnología de intercomunicación masiva. A principios del siglo XXI, se habla sobre la existencia de dos fuerzas que dan forma al mundo actual, la tecnología y la globalización. Una aproximación podría tomar a la tecnología como herramienta para determinar las preferencias humanas y su gestión y a la globalización como fuente de las realidades económicas actuales y su desarrollo [Thomas 2005].

En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo distancia y velocidad), las organizaciones tiene que ser más competitivas y poder sobrevivir con el uso de las TI y de la información.

Dicho uso creciente de la tecnología de la información por parte de las organizaciones conlleva también a una mayor dependencia hacia ella y por lo tanto, los riesgos relacionados a las tecnologías de la información se transfieren a los

procesos del negocio; lo cual, involucra una responsabilidad para la Alta Dirección respecto a la administración de los riesgos relacionados con la tecnología de información, ya que el no hacerlo podría poner en riesgo la seguridad de uno de sus activos más importantes: la información, los productos o servicios ofrecidos y la continuidad de sus operaciones.

Las tecnologías de la información se han adoptado y aplicado por los países de todo el mundo como un medio para mejorar el desempeño del gobierno. Además de una amplia gama de nuevas prácticas de gestión pública, tales como la descentralización, la gestión del rendimiento y el gobierno electrónico.

Los retos de la administración de la seguridad de la información son enormes en los momentos actuales y serán aún mayores conforme vaya evolucionando a sistemas más complejos y sofisticados por el uso intensivo de las TI. Por ello la seguridad es parte fundamental de las iniciativas de Gobierno Electrónico a nivel mundial. Por lo que, "los estándares son esenciales en tales circunstancias para proveer un sistema de seguridad de la información, definición de los requisitos, alcance, políticas, métricas de gestión, monitoreo y evaluación del sistema" [Stallings 2007].

Los gobiernos nacionales han reconocido las TI basadas en la Web como una parte importante de acercamiento a los ciudadanos desde principios de 1990. "El gobierno electrónico" ha sido la innovación más importante; su aparición se puede remontar a 1993 con el informe de reingeniería de Tecnologías de la Información, que formaba parte de la revisión de rendimiento nacional a principios de los años de gobierno de Bill Clinton (Lenk y Traunmüller 2002). Quien reinventar el gobierno norteamericano mediante la creación de una administración más eficiente, menos costosa y con resultados significativos. [Kamensky, 1999]. Por una parte, se trataba de vincular a los ciudadanos con los órganos del gobierno para que pudiesen obtener servicios automatizados; por otra, se deseaba que el gobierno redujera costos, mejorara su rendimiento y aumentara su velocidad en la entrega de servicios mediante la implementación y conexión a través de redes de información y comunicación [Almarabeh+ 2010].

Para ello, resultaba imprescindible el uso selectivo de las tecnologías de información y comunicación; de manera particular internet. La amplia aceptación de la idea de Clinton, aunada a la rápida expansión del World Wide Web (www) en los años noventa, dio lugar a lo que hoy conocemos como gobierno electrónico o e-gobierno.

Para entender el gobierno electrónico, hay que remontarse al origen de Internet en 1969, cuando el Departamento de Defensa de los Estados Unidos comenzó el proyecto ARPANET, "un sistema de conexión digital que conectaba a varias computadoras en diferentes ubicaciones geográficas" [West 2007].

Sin embargo, no fue sino hasta 1991, con la formación de la WWW, interface integrada por el uso, envío y manipulación de textos, imágenes y sonidos, que Internet se estableció como un medio de comunicación general. Años después, las agencias gubernamentales descubrirían que la "red" era un medio útil para comunicarse con los ciudadanos, empresas y otros organismos sociales, debido a la posibilidad de publicar y amplificar su información y ofrecer en línea algunos servicios, así como ampliar y poner a disposición sus contenidos a un amplio grupo de personas.

Los recientes informes sobre el desarrollo del gobierno electrónico revelan diferentes patrones de implementación (Ebbers y Van Dijk 2007; Rose, 2005; West 2005), incluyendo una seria brecha digital que existe en todo el mundo entre los países desarrollados y en desarrollo de las Naciones Unidas (2006), Conocida como brecha digital [Chung-pin+2011].

Estimulado por este informe y la revolución simultánea en gestión de calidad, los gobiernos de los Estados Unidos, Gran Bretaña, Europa, Taiwán y Australia emergieron como líderes en la implementación de aplicaciones de gobierno electrónico (Lee, Tan, y Trimi 2005). Muchas instituciones como las Naciones Unidas (ONU), el Banco Mundial, y los investigadores de la Brown University y la Universidad de Rutgers (Newark), han comenzado la recolección de datos empíricos para investigar y comparar el rendimiento del e-gobierno en las ciudades y países del mundo [Chung-pin+2011].

El gobierno electrónico es una herramienta esencial en materia de gobierno, al punto que ha obligado "a repensar organizaciones, responsabilidades, procesos de negocios y acuerdos de colaboración y de cooperación dentro y entre los niveles de gobierno" [OECD 2008].

El gobierno electrónico incluye aplicaciones informáticas para transformar las relaciones tanto internas como externas (ONU, 2003). Las relaciones internas se refieren a las interacciones entre organismos dentro del gobierno, mientras que las relaciones exteriores se centran en el uso de aplicaciones basadas en internet para la mejor prestación de servicios y consulta pública sobre la información del gobierno [Chung-pin+2011].

De acuerdo con West (2007) existen cuatro etapas en las que se desarrolla el gobierno electrónico:

- La de cartelera es la primera etapa se asemeja a un cartel anunciador con información del gobierno y se caracteriza por mostrarla en un sentido estático, donde es imposible la comunicación de doble vía entre funcionarios públicos y ciudadanos, ya que exclusivamente se divulgan reportes, publicaciones y bases de datos; por ello se llama etapa de cartelera.
- La prestación parcial de servicios es la segunda etapa, los ciudadanos pueden acceder, clasificar y buscar bases de datos e información, y si bien hay ciertos servicios en línea, éstos tienden a ser esporádicos y limitados para algunas áreas; asimismo, a los ciudadanos no les es posible personalizar el sitio ni participar en conversaciones con funcionarios. En este estadio, la necesidad de llamar o visitar las oficinas de gobierno por parte de los ciudadanos disminuye gracias a la posibilidad de acceder a la información y los contenidos en línea; además, la capacidad de ver los informes de gobierno y bases de datos ayuda a los ciudadanos a entender el desempeño del quehacer del sector.
- La prestación de servicios en línea totalmente ejecutables e integrados al sitio web, lo cual mejora la habilidad de los ciudadanos y empresas para encontrar información y ordenar servicios. Es en esta etapa donde se coloca la publicación de políticas de privacidad y seguridad.

- La democracia interactiva con alcance al público y con características para la mejora en transparencia y rendición de cuentas es la última etapa, está integrada por servicios completamente ejecutables en línea, opciones para la personalización del sitio web de acuerdo a los intereses particulares del ciudadano, así como la recepción de suscripciones electrónicas con actualizaciones automáticas de temas o áreas específicas de interés individual.

No es realista pensar que la construcción del gobierno electrónico constituya un proceso básicamente técnico, sino que requiere ser abordado de una manera comprehensiva, en la que los procesos y las personas constituyan el centro de atención, es decir entender los servicios públicos desde un punto de vista multidimensional, donde se distingue:

- El marco estratégico, que dirige la atención a los requerimientos organizacionales básicos;
- El nivel de los servicios públicos, los procesos y el flujo de trabajo, donde las estrategias y los papeles básicos adquieren contenidos;
- El nivel de interacción, donde la atención se concentra en el desempeño del servicio;
- El nivel de tecnologías de la información, que se refiere a la implementación técnica de los componentes del proyecto, formatos estándares de intercambio de información, la comunicación, la infraestructura de transacción y transporte con sus interfaces.

Entre las limitaciones más relevantes para la implementación del gobierno electrónico, destaca la capacidad de cambio y adaptación de nuevas tecnologías por parte de las agencias gubernamentales, condicionada por factores como la existencia de múltiples sistemas de prestación de servicios, la fragmentación burocrática, las restricciones presupuestales, los conflictos de grupo y los diversos liderazgos [West 2007].

Las Naciones Unidas a través de su unidad de administración pública desde el 2003 elabora cada 02 años la encuesta sobre gobierno electrónico y nos acaba de presentar la encuesta del 2014. El informe considera 03 componentes de medición (Servicio en línea, Telecomunicaciones e Infraestructura y Capital humano), de los cuales en lo

correspondiente a servicios en línea se consideran los siguientes temas: la prestación de servicios en línea enfocada en la adopción global del gobierno, la prestación de servicios multicanal, reducir la brecha digital, gobierno abierto (transparencia) acercándonos a las poblaciones vulnerables y al mayor uso del gobierno electrónico para aprovechar sus beneficios.

A nivel de continentes, se revela un avance significativo en Europa seguido de América sobre el promedio mundial, Asia en el promedio y Oceanía y África debajo del promedio. Respecto a los países, la lista está encabezada por la República de Corea, seguido de Holanda, Reino Unido, Dinamarca y Estados Unidos, entre los cinco primeros. En los 20 primeros puestos considerados como líderes no está presente ningún país latinoamericano, sin embargo, figuran Chile y Colombia como nuevos países emergentes en gobierno electrónico (ver Cuadro 1.1).

País	2010	2012	2014
Chile	34	39	33
Colombia	31	43	50
Uruguay	36	50	26
Argentina	48	56	46
Brasil	61	59	57
Venezuela	70	71	67
Perú	63	82	72
Ecuador	95	102	83

Cuadro 1.1 Ranking en América Latina y el Caribe. **[UNITED NATION 2008 - 2014]**

En el Perú la Presidencia de Consejo de Ministros mediante RM N° 274- 2006-PCM aprobó la Estrategia Nacional de Gobierno Electrónico, así como en el Portal Electrónico de la Comisión Multisectorial para el seguimiento y evaluación del "Plan de Desarrollo de la Sociedad de la Información", como parte del desarrollo del gobierno electrónico, meta incluida en la matriz del Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana aprobado mediante DS N° 031-2006-PCM.

La visión establecida para la Estrategia Nacional de Gobierno Electrónico es la "Transformación de las relaciones del Estado Peruano con empresas privadas, instituciones públicas y ciudadanos, mediante el uso efectivo de la tecnología de la información y comunicaciones, haciendo que el Estado en su conjunto se organice, estableciendo una red de servicios transaccionales y de información acordes con las necesidades y demandas de la sociedad, y que conlleven al bienestar general".

Sin embargo, como se puede apreciar en la encuesta de gobierno electrónico realizada por la unidad de administración pública de las Naciones Unidas, respecto a los datos del Perú, se observa un claro retroceso, principalmente porque pasamos del puesto 53 de la encuesta del 2014 al puesto 72 en esta última encuesta. Es decir, descendimos 19 puestos. Pero esta tendencia no es distinta a las encuestas pasadas, puesto que, de haber estado en el puesto 53, en los años 2003 y 2004, pasamos al puesto 56, retrocediendo 3 puestos en el 2005 y avanzando un puesto en el 2008. Lo más lamentable es que no hemos avanzado significativamente desde el 2008, donde empieza nuestra tendencia a la baja, retrocedimos del puesto 55 al 63 en el 2010 (ver Cuadro 1.2).

Perú	2003	2004	2005	2008	2010	2012	2014
Puesto	53	53	56	55	63	82	72

Cuadro 1.2 Encuestas sobre gobierno electrónico en Perú. **[UNITED NATION 2008 - 2014]**

Más allá de ver nuestro puesto dentro del ranking mundial, los resultados llaman a cuestionarse: ¿Por qué nos quedamos?, ¿Por qué retrocedimos tanto? o ¿Qué está fallando? y finalmente a nivel latinoamérica somos el país que más ha retrocedido, ¿A qué se debe el éxito de los demás países?, ¿Son sus políticas?, ¿Tiene que ver con la posición de los organismos rectores de estas políticas dentro de la estructura del Estado y por ende es un factor de liderazgo? y ¿El Poder político y la habilidad para agendar estos temas tiene que ver con un factor de recursos económicos y humanos?

1.2 Formulación del Problema

El gobierno electrónico depende del adecuado funcionamiento y uso de las tecnologías de la información en la gestión inter-organizacional del Estado y los servicios e información ofrecidos a los ciudadanos.

Un elemento crítico para el éxito de las organizaciones es la administración efectiva de la información y de las TI relacionadas [Jiang+ 2000]; complementariamente, se ha identificado que la cooperación es un elemento clave en las compañías más exitosas del mundo ya que crea sinergia, innovación, productividad, creatividad y entusiasmo [Gratton 2008].

En el Perú los lineamientos y orientación para la implementación de la seguridad de la información y el gobierno electrónico están a cargo de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), la cual desde el 2004 a través de la Presidencia de Consejo de Ministros ha establecido la obligatoriedad de implementar seguridad de la información en todas las entidades integrantes del Sistema Nacional de Informática.

Sin embargo, pese a los esfuerzos realizados, la encuesta de gobierno electrónico realizada por la unidad de administración pública de las Naciones Unidas, muestra que pasamos del puesto 53 en el año 2003 al puesto 72 en el 2014, es decir, descendimos 19 puestos y de acuerdo a la ONGEI desde el 2004 al 2015 solo 03 de aproximadamente 2000 entidades integrantes del Sistema Nacional de Informática han implementado seguridad de la información en procesos diferentes a los de servicio de e-gobierno.

Asimismo, no hay un entendimiento claro sobre la responsabilidad global de seguridad de la información dentro de la institución, lo cual se refleja en que el nivel de liderazgo para la implementación mayormente descansa en los gerentes o jefes de áreas de informática y sin el compromiso de la alta dirección, con enfoque de seguridad informática más que a la seguridad de la información [Mariño 2010].

En este contextos, el principal problema es que no se cuenta con un modelo de gestión de seguridad de la información que orienten la implementación y supervisión de la seguridad de la información en los servicios de gobiernos electrónico brindado por las entidades del sector público, por lo cual pese a la obligatoriedad de la implementación de la norma de seguridad de la información y a la inversión realizada en tecnologías de información, continúa siendo mínima la implementación de seguridad de la información, observándose lo siguiente:

- No se ha definido un estructura organizacional con roles y responsabilidades que permita orientar la gestión de seguridad de la información.
- Se desconoce el nivel o la necesidad de seguridad con la que debe contar la información para el tratamiento que se realiza de acuerdo a las relaciones y fase del gobierno electrónico.
- Inexistencia de controles de seguridad o con vulnerabilidades para el almacenamiento, procesamiento y transferencia de la información requerida en los procesos de la organización.
- No se cuentas con indicadores y métricas que permitan realiza el monitoreo de los controles o medir el nivel de eficiencia de estos.

Dicha problemática de seguridad de la información para el gobierno electrónico genera que no se pueda tener una buena gestión organizacional, inter-organizacional, ni brindar efectivamente los servicios de información ofrecidos a los ciudadanos.

Este conjunto de elementos hace especialmente interesante un trabajo de investigación sobre el impacto de la gestión de seguridad de la información en el nivel y fase de implementación del Gobierno electrónico.

En dicho sentido, la presente investigación busca identificar el grado de influencia que la seguridad de información tiene sobre la implementación del Gobierno electrónico en el Estado Peruano.

1.3 Justificación

La justificación teórica y práctica se define a continuación:

1.3.1 Aporte Teórico

Definir un Modelo de Gestión de Seguridad de la Información para el Gobierno Electrónico en el estado, que establezca una estructura organizacional de la seguridad, niveles de madurez, controles, indicadores y métricas, con la finalidad que permita implementar, gestionar y monitorear la seguridad de la información en los diferentes servicios del gobierno electrónico brindado por las entidades del estado.

1.3.2 Aporte Práctico

Este proyecto busca contribuir en identificar la importancia de la gestión de la seguridad de la información en el desarrollo del gobierno electrónico y contar con un modelo de gestión de seguridad que permita monitorear su implementación reduciendo el impacto potencial que pueden ocasionar los riesgos.

Es importante resaltar que este trabajo trata un tema asociado a la realidad actual de las organizaciones y que cuyo resultado podrá servir como orientación para otras que quieran tener una participación más activa en el gobierno electrónico.

Esta investigación es necesaria para la alta dirección y el personal de las organizaciones, porque les va a brindar aportes en formas de apreciaciones, conclusiones y recomendaciones de acciones correctivas o preventivas que les pueda servir para comprender y mejorar la gestión del riesgo de seguridad de la información en sus organizaciones, lo cual les va a permitir contar con un sistema de gestión de seguridad de la información con niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información considerados relevantes para la entidad, de manera tal que se asegure la continuidad

operacional de los procesos y la entrega de productos y servicios a los usuarios, clientes o beneficiarios.

De esta manera se pueda lograr implementar el modelo seguridad de la información para el gobierno electrónico y obtener beneficios como:

- Mayor eficiencia.
- Menor costo para ofrecer los servicios.
- Rapidez y agilidad para obtener el servicio o producto requerido.
- Accesible de cualquier parte.
- Mayor compenetración con el ciudadano.
- Ventanilla única que proporciona información en línea 24 horas al día y permite el autoservicio en una forma amigable.

Además de estos beneficios, implementar los componentes de gobierno electrónico permite que el Estado y la sociedad puedan beneficiarse en lo siguiente:

- Tener mayores satisfacciones en el trabajo, esto hace que los servidores públicos tengan más productividad y con ello mayor retención de la gente capaz.
- Un mayor crecimiento económico e impulso del sector privado para invertir en soluciones de negocio para la organización y para el ciudadano.
- El uso de servicios en línea también facilita la participación electrónica con el gobierno.

1.4 Objetivos

1.4.1 Objetivo General

Elaborar un modelo de gestión de seguridad de la información para el gobierno electrónico en las entidades públicas.

1.4.2 Objetivos Específicos

a) Definir la estructura organizacional y las funciones de los responsables de la seguridad de la información.

b) Identificar y establecer niveles de madurez de seguridad de la información.
c) Establecer controles de acuerdo al nivel de madurez requerido en los procesos que brindan servicio de gobierno electrónico.
d) Establecer métricas e indicadores que permitan medir el desempeño de los controles y la gestión de seguridad en los servicios del gobierno electrónico.

2 CAPITULO II: ESTADO DEL ARTE

2.1. Revisión de la Literatura

2.1.1. Modelo Sistémico de la Seguridad de la Información en las Universidades [Viloria, 2009]

Este modelo gerencial se base en un estudio realizado en las universidades de Venezuela, cuyo objetivo es brindar un marco conceptual que contribuya a elaborar planes estratégicos para abordar el problema de la inseguridad de la información. Dicho modelo incorpora herramientas de las organizaciones inteligentes presentes en cada subsistema de la quinta disciplina.

2.1.2. Modelo de Madurez de la Seguridad de la Información en el Contexto de las Organizaciones Inteligentes. [Marianela Villegas+ 2009]

Esta investigación presenta un modelo de madurez en el contexto de las cinco disciplinas de las organizaciones inteligentes de Peter Senge: el dominio personal, los modelos mentales, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico; cuyo objetivo es disminuir la complejidad y la incertidumbre en la gestión de la seguridad de la información, para lo cual propone un modelo de madurez integrado por cinco niveles: inicio, crecimiento, desarrollo, madurez e inteligencia.

2.1.3. Practical Application of Information Security Models. [Vladimir, 2011]

El autor plantea un modelo denominado Modelo de Seguridad GRC (Gobierno, Riesgo y Cumplimiento) cuyo propósito es ayudar a entender ¿por qué la seguridad es importante? y soportar la justificación de qué tan costoso es la tecnología que queremos implementar, dependiendo del punto de vista de la política de seguridad, y el apetito al riesgo empresarial, para lo cual es importante el entendimiento o compatibilidad de la gestión de riesgos de seguridad de la información con los objetivos del negocio y de los profesionales de seguridad con los líderes o gerentes del negocio.

2.1.4. Modelo de Seguridad de la Información en TIC. [Burgos 2011]

El modelo plantea una estructura basada en la implementación práctica y concreta relación con las actividades, bajo dos grandes fases (Elaboración y Aplicación) que permiten dar seguridad a la organización, la cual de acuerdo a sus propias necesidades, lineamientos y perspectivas de negocio, busca mantener su información asegurada.

El modelo se apoya en el análisis de las normas y estándares internacionales relacionados con la seguridad de la información y considera los principales elementos incluidos en estas, cubriendo temas de seguridad y de riesgos, así como, apoyando a lograr aspectos de estructura organizacional y descripciones de cargo y tareas.

2.1.5. Towards an Information Security Maturity Model for Secure E-Government Services: A Stakeholders View. [Karokola, 2011]

El modelo de madurez de seguridad de la información (ISMM) está diseñado para asegurar los servicios de gobierno electrónico (aplicación y prestación de servicios) de manera integral, que aborde aspectos de seguridad tanto técnicos como no técnicos, permitiendo medir tanto la calidad como la cantidad de los servicios del gobierno electrónico.

2.1.6. Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea 2.0. [MINTIC, 2011]

Este modelo plantea una estructura organizacional de seguridad, la cual se apoya en un Sistema de Administrativo de Seguridad de la Información de Gobierno en Línea (SASIGEL). Asimismo, el modelo alinea las políticas de seguridad con normas y mejores prácticas de la industria (NTC – GP100, MECI e ISO 27001), agrupa y determina el tipo de controles a implementar por las entidades destinatarias del servicio en línea y define niveles de madurez de los controles, con la finalidad de mantener un ambiente razonablemente seguro que permita proteger los activos de información que componen la estrategia de gobierno en línea.

2.1.7. O-ISM3: Open - Information Security Management Maturity Model. [The Open Group, 2011]

El O-IMS3 es un estándar orientado a procesos que ofrece un enfoque cuantitativo para evaluar la gestión de un sistema de seguridad de la información en una organización, debido a que establece niveles de madurez sobre 04 modelos conceptuales (gestión, organización, sistema de información y seguridad contextual) y la aplicación de métricas para administrar los procesos de seguridad de la información.

2.1.8. Las Métricas, Elemento Fundamental en la Construcción de Modelos de Madurez de la Seguridad Informática. [Villegas, 2011]

Este modelo se basa en el modelo contextualizado de colado & Franco al que le define e incorpora la funcionalidad de las condiciones de seguridad informática, de tal manera que permita establecer los principales indicadores de seguridad y agruparlos en los 4 niveles establecidos para poder medir el desempeño de la entidad frente a los retos que plantea la preservación y resguardo informático.

2.1.9. Sistema de Gestión de Seguridad de la Información. [ISO, 2013]

Esta modelo plantea requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información estructurado en clausulas, objetivos y controles. Dicho

modelo debe ser implementado por las organizaciones de acuerdo a sus necesidades y objetivos.

La ISO/IEC 27001 es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información y proporcionan un marco de gestión utilizable por cualquier tipo de organización, pública o privada, grande o pequeña, basada en un enfoque de procesos.

2.1.10. Directiva de Seguridad de la Información para la Protección de Datos Personales. [APDP, 2013]

La directiva es un instrumento que facilita la adopción de la seguridad de la información para la protección de los datos personales, para lo cual propone responsabilidades y medidas de seguridad jurídicas y técnicas referidas a los controles para asegurar la confidencialidad, disponibilidad e integridad de la información.

2.1.11. Guía Metodológica – Sistema de Seguridad de la Información en el Programa de Mejoramiento de la Gestión y Metas de Eficiencia Institucional. [DIPRES, 2014]

Este modelo plantea una estructura organizacional, etapas, dominios y actividades detalladas para el desarrollo de cada uno de los requisitos de seguridad de la información, así como una propuesta de indicadores de desempeño, con la finalidad de que las instituciones implementen un sistema de seguridad de la información facilitando a los servicios públicos verificar el cumplimiento de los objetivos comprometidos.

2.2. Descripción de Modelos de Seguridad de la Información

2.2.1. Modelo Sistémico de la Seguridad de la Información en las Universidades (MOSSIU).

Es un modelo extendido del MDO de leavitt (Estructura, Tecnología, personas y tareas), pero bajo un enfoque de la seguridad de la información en el contexto de una organización inteligente.

El modelo plantea que es importante comprender las relaciones existentes entre los componentes que intervienen en la seguridad, caso contrario no habrá valor agregado en las organizaciones (ver Figura 2.1).

Figura 2.1 Relaciones entre los componentes que intervienen en la seguridad. **[Viloria, 2009]**

A continuación se detalla cada uno de los componentes del MOSSIU

a) La gente y la cultura de la seguridad de la información.

La cultura en seguridad de la información es una subcultura de la cultura organizacional, puede definirse como: el conjunto de valores éticos y actitudes, las tradiciones, creencias, hábitos, modelos mentales, la visión, las normas, los procedimientos, todo lo que permita identificar la madurez de la institución en la administración de la seguridad de la información y sobre todo alcanzar los objetivos, la misión y la visión de la institución bajo una perspectiva de seguridad de todos sus bienes informáticos.

En este subsistema los trabajadores del conocimiento cuya función es la de garantizar la Seguridad de la Información (SIF), observan la problemática de la inseguridad bajo una perspectiva sistémica, igualmente poseen un alto dominio personal. Los equipos de desarrollo de software y de soporte técnico participan, colaboran, dan valor agregado al conocimiento, redefinen tareas, y asumen responsabilidades para alcanzar la visión enmarcada en la SIF. En resumen, la visión compartida enfocada en la SIF es notoria, es una fuerza que estimula a todos los trabajadores del conocimiento y de oficina a crear nuevas actitudes y aptitudes (Dominio Personal) para afrontar y reducir los problemas de inseguridad de la información en la organización, en efecto, es un proceso de aprendizaje continuo. En la cultura de la SIF del MOSSIU, la disciplina del dominio personal es un proceso que permanece en el tiempo, el conocimiento se expande siempre para alcanzar los objetivos.

b) Las TIC y sus capacidades.

Las TIC forman parte de los sistemas de información de las universidades, sus herramientas son usadas para desarrollar aplicaciones, almacenar datos e información, proteger los bienes informáticos, además poseen capacidades computacionales y de comunicación, un ejemplo es toda la infraestructura tecnológica que soporta a una intranet o extranet universitaria.

Por otra parte, la adopción de una red privada como una intranet o extranet universitaria o la implantación de un sistema de información, trastoca el equilibrio aparente de una institución, aumenta la entropía en todos los subsistemas que integran el MDO de Leavitt, por ello es necesario implementar una serie de estrategias en cada elemento de este modelo, así el sistema se auto-organiza y evoluciona a otra estructura más compleja. Adicionalmente aparecen otros problemas, no contemplados en el modelo de Leavitt que exigen la instrumentación de otros cursos de acción para tratar de controlarlos y minimizarlos, este escenario lo contempla el MOSSIU, este modelo abarca las redes privadas, los servicios de salvaguarda, los mecanismos y herramientas de seguridad y sus capacidades.

En este subsistema se identifican, sin restricción, las medidas de protección de los activos informáticos con la intención de reducir el riesgo intrínseco, se instrumentan metodologías para identificar las funciones y los servicios de seguridad, se agrupan activos y sus amenazas, se determina el riesgo, y se proponen herramientas y mecanismos de seguridad. Todas las actividades señaladas nunca terminan, son repetitivas e iterativas, debido a los nuevos activos informáticos que deben ser protegidos y los diversos cambios del contexto organizacional, lo que induce a que aparezcan nuevas amenazas y modalidades de ataques.

c) La estructura organizacional de la seguridad de la información.

La estructura organizacional en el MOSSIU, al igual que en el MDO de Leavitt, cambia. En el MOSSIU evoluciona la estructura interna con la finalidad de que los trabajadores del conocimiento y de oficina se acoplen con las formas de realizar las tareas y los procesos como consecuencia de los desajustes producidos por adoptar la tecnología. Es importante destacar que este esquema separa las TIC de otras tecnologías existentes en la organización, ya que las TIC son el eje central que enlaza a todo la empresa (Viloria y Blanco, 2006c).

Esta característica de las TIC, en especial de las redes privadas dispara la entropía en la universidad, pues los efectos colaterales afloran en cualquier momento y algunos permanecen ocultos después de adquirir la tecnología, surgen nuevas vulnerabilidades y aumenta la inseguridad de la información. Por ello en este subsistema es importante la existencia de una unidad organizacional de la SIF que abarque la seguridad física y lógica. Asimismo, en este componente del MOSSIU entra en juego nuevamente la disciplina del aprendizaje en equipo y evidentemente para comprender la situación que es compleja, el pensamiento sistémico.

Esta unidad organizacional posee una visión compartida bajo una perspectiva de la SIF, pero creada por los equipos de trabajo, encargados de la seguridad.

Por otro lado, en este componente existen los códigos de cargos administrativos asociados al rol que cumplen los encargados de la SIF, un ejemplo puede ser: un encargado de la seguridad lógica I o un encargado de la seguridad física II, denominaciones que dependen del dominio personal logrado por los trabajadores del conocimiento en la SIF. Deben incluirse los programas de incentivos socio económicos, pues los empleados con una alta experticia en SIF son muy bien remunerados en el mercado laboral, de esta manera se podría contribuir a mantenerlos en la institución.

d) Procesos y tareas bajo una perspectiva de la SIF.

Los procesos pueden estar integrados por varias unidades organizacionales que interactúan a través de la información, asimismo por la propiedad de recursividad de los sistemas, sus componentes son otros subsistemas, en donde aparecen otros elementos, como personas, computadoras, redes, bases de datos, aplicaciones, entre otros. Bajo otra perspectiva, un proceso es la ejecución de un conjunto de tareas en donde se manejan datos e información con la finalidad de lograr un objetivo. Esta teorización

conceptual evidencia que el componente procesos y tareas tiene una fuerte relación con los otros elementos del MDO de Leavitt, como la cultura y la gente, las tic y sus capacidades, y la estructura organizacional.

En el componente: los procesos y las tareas bajo una perspectiva de la SIF del MOSSIU, la aplicación de procedimientos de seguridad son vitales para blindar a los procesos y las tareas y proteger la información y los datos, se definen de acuerdo a las características del negocio y las TIC necesarias para instrumentar las políticas de seguridad de la información(PSI) (Viloria y Blanco, 2006), por ello existe una fuerte relación sistémica con los otros componentes del modelo, la cultura por las PSI, las TIC por las herramientas y mecanismos de seguridad y sus capacidades así como la estructura organizacional por el rol que juega la unidad organizacional de la SIF para proteger los activos informáticos involucrados en los procesos. En tal sentido, en este modelo se asume que los equipos de trabajo tienen bien definida la visión compartida y poseen un alto dominio personal, además los modelos mentales se alinean con las disciplinas de las organizaciones inteligentes y el problema de la inseguridad informática se analiza bajo el pensamiento sistémico.

2.2.2. El Modelo de Madurez de la Seguridad de la Información en el Contexto de las Organizaciones Inteligentes (MMASI)

Este modelo se encuentra integrado por cinco niveles de madurez a ser adoptado por las organizaciones inteligentes como un factor crítico de éxito (ver Figura 2.2).

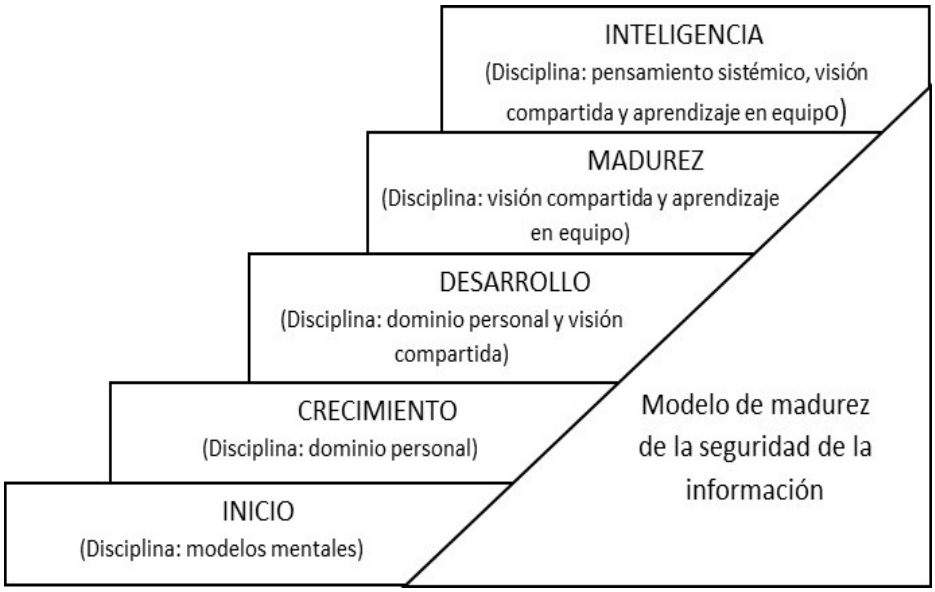


Figura 2.2 MMASI en el contexto de las organizaciones inteligentes. **[Marianela Villegas+ 2009]**

A continuación se describe cada uno de los niveles:

a) Nivel de inicio.

   Es el primer nivel del modelo MMASI, en donde las organizaciones no producen las acciones necesarias y suficientes para proporcionar un aprendizaje bajo un sentido de Seguridad de la Información. Existen altos niveles de anarquía en la adopción de medidas básicas de seguridad, cada usuario instala herramientas de software y hardware en su computadora, sin estar alineado a ningún plan de seguridad.

   Los modelos mentales que sesgan las decisiones y producen soluciones erróneas predominan entre los encargados de la seguridad de la información, un ejemplo es considerar al personal técnico como el único responsable de la seguridad (Morales, 2004; Viloria y Blanco, 2006).

   Conclusión: no hay actitudes proactivas sino reactivas, por lo tanto no se aplica la disciplina del dominio personal, tampoco hay presencia de las otras disciplinas de las organizaciones inteligentes.

b) Nivel de crecimiento.

Es el segundo nivel del modelo MMASI, todavía no se han superado muchos de los problemas y situaciones presentes en el nivel de inicio; aún existe una barrera en la comunicación entre la alta gerencia y el departamento de sistemas o afines.

Destacan las siguientes características:

- Encargado de la seguridad de la información.
- Medidas de seguridad básicas.
- Herramientas básicas de hardware y software.
- Backups y recuperación de datos.

Surge la preocupación de que la seguridad es un problema de todos, que amerita atención. Se toma conciencia de las debilidades actitudinales y de las incompetencias de los trabajadores de la seguridad, en otras palabras, comienza a desarrollarse el dominio personal. Por otro lado, persiste cierto ambiente de anarquía, por la instalación del software propietario y libre, sin estar enmarcado en ningún plan de seguridad.

c) Nivel de desarrollo.

Es el tercer nivel del MMASI, existe una visión más amplia y sistémica de seguridad de la información, aumenta la preocupación por el problema de la inseguridad de los activos informáticos. Cambia la estructura organizacional, se crea el departamento o unidad encargada de la gestión de Seguridad de la información con sus respectivos gerentes y personal adscrito con experticia en el área, dedicados exclusivamente a las actividades concernientes a la seguridad física o lógica.

Destacan las siguientes características:

- Unidad organizacional o departamento de la seguridad de la información.

- Documento de seguridad de la información.
- Valores y conductas éticas.
- Medidas de seguridad intermedias.
- Difusión de las políticas de seguridad de la información.
- Registro de eventos.
- Implantación de la seguridad lógica.
- Seguridad física.

Predomina la actitud proactiva ante la reactiva, el dominio personal se fortalece, se instauran grupos consolidados de seguridad con una visión compartida.

d) Nivel de madurez.

Es el cuarto nivel del modelo MMASI se caracteriza por tener los siguientes indicadores:

- Sistema de activos informáticos.
- Adopción de las políticas de la seguridad de la información.
- Desarrollo de un plan estratégico.
- Auditorías internas y externas.
- Medidas de seguridad avanzadas.
- Adopción de los valores éticos.
- Visión compartida.
- Trabajo en equipo.

Los equipos de trabajo de seguridad de la información trabajan en conjunto, generan sinergia y están bajo una visión común de ésta, estimulados por la aceptación colectiva de modelos mentales compartidos. La organización resalta muchas características que le permite generar conocimiento.

e) Nivel de inteligencia organizacional

Este nivel se caracteriza por tener los siguientes indicadores:

- Cultura organizacional de la seguridad de la información.

- Desarrollo de aptitudes y actitudes.
- Análisis y gestión de riesgo.
- Ejecución del plan estratégico.
- Monitoreo permanente a los activos informáticos.
- Responsable de las políticas de la seguridad de la información.

En virtud de los indicadores descritos, la empresa alcanza su máximo nivel de madurez, es una organización que aprende a aprender, la cultura de la seguridad está arraigada, las disciplinas de las organizaciones inteligentes son aplicadas en el ámbito organizacional de la seguridad de la información. La relación sistémica entre las disciplinas se encuentra en un nivel que genera sinergia, la cual se manifiesta en los procesos que se activan a raíz de ataques hacia los activos informáticos. Estos procesos están sustentados en todo el conocimiento producido por la organización, ya que los grupos encargados de la seguridad por trabajar en equipo y poseer un alto dominio personal, manifiestan que les permite tomar decisiones proactivas.

En otras palabras, la organización responde con más eficiencia y efectividad a los embates del medio interno y externo que trastocan el equilibrio dinámico de la organización (Leavitt, 1965, Blanco y Viloria, 1999) llevándolo a un estado de mucha entropía (Briggs y Peat, 1999) y por otro lado la lleva rápidamente a su equilibrio aparente (Viloria y Blanco, 2006).

El modelo MMAGSI en el contexto de las organizaciones inteligentes tendría como:

✓ Estrategia, una dirección y un equipo de empleados conscientes del problema de la inseguridad de la información, de sus fortalezas y debilidades; para definir una misión, visión y objetivos en términos de conocimiento previos en seguridad de la información.

- ✓ Infraestructura, que incluye los procesos organizativos de la empresa y las tecnologías de la información como mecanismos acordes para facilitar la creación y el intercambio del conocimiento.
- ✓ Gestión de personal, que es el pilar clave de toda la gestión del conocimiento y está ligado a los aspectos culturales de la organización.

2.2.3. Practical Application of Information Security Models (MGRC).

El modelo está compuesto por tres áreas: conductores de la seguridad, gestión de la seguridad y las partes interesadas (ver Figura 2.3).

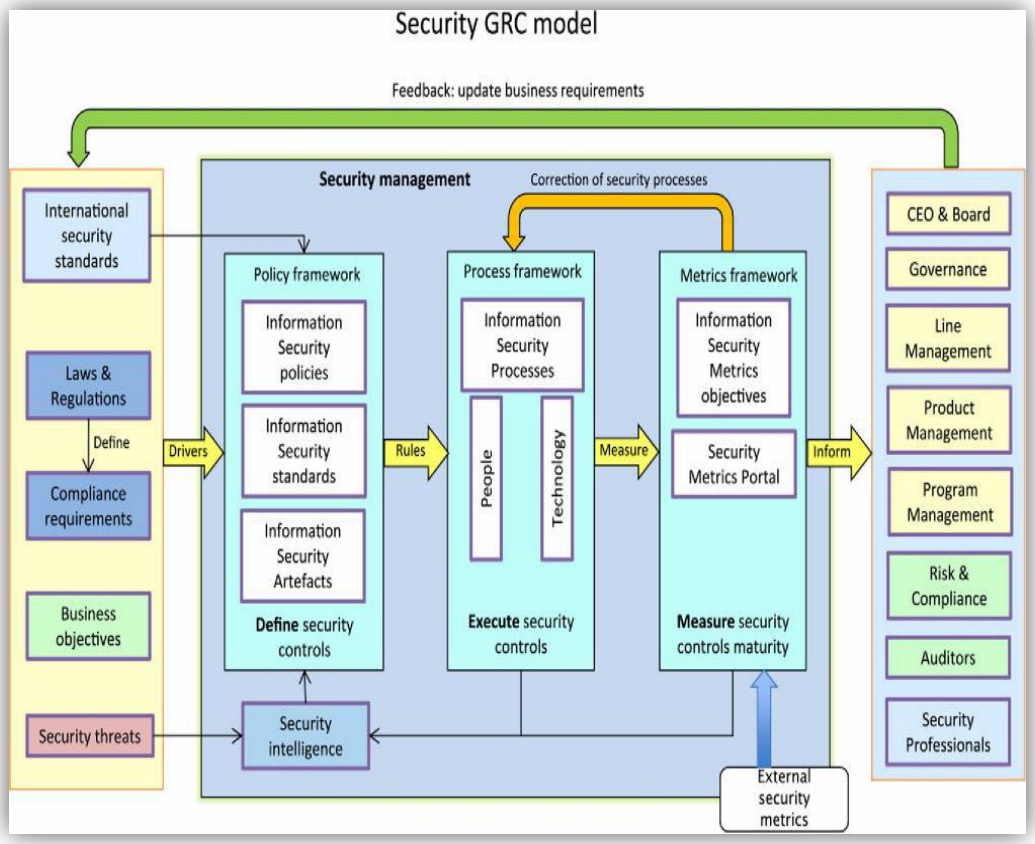


Figura 2.3 Modelo de seguridad GRC. **[Vladimir, 2011]**

a) Conductores de la seguridad.

Está claro que sin conductores entonces no necesitaríamos ningún tipo de seguridad.

Hay tres conductores principales de trabajo de seguridad:

1. Leyes y reglamentos.

   Son algo más que una empresa debe cumplir o enfrentar una acción legal o multa.

2. Los objetivos de negocio.

   La empresa típicamente busca generar ganancias y define un conjunto de objetivos de negocio; la seguridad apoya estos objetivos de negocio mediante la protección de los sistemas y la información que se utiliza en los procesos de negocio.

3. Amenazas de seguridad.

   Trabajan en contra de las leyes, regulaciones y objetivos de negocio.

b) Gestión de la seguridad (la parte principal)

En esta área contamos con tres marcos que permiten a la empresa alcanzar los objetivos definidos en la sección de los conductores.

1. Marco de políticas.

   Se trata de un conjunto de políticas, normas y directrices que describen cómo la empresa realiza el tratamiento de los conductores de seguridad de la información.

2. Marco de procesos.

   Cualquier control de la seguridad en una política o estándar es un proceso, no hay excepciones. Cada proceso es apoyado por la gente y la mayoría están soportados por la tecnología. Sin embargo, es necesario que haya alguna relación entre la tecnología que tiene la empresa, sus procesos y el control correspondiente en el marco de la política hasta el objetivo del negocio. Esto permite la trazabilidad de las inversiones en

seguridad y a los profesionales de la seguridad justificar los presupuestos de seguridad.

3. Marco de métricas de seguridad.

   Una declaración difundida que se puede aplicar en la seguridad es "Lo que no se puede medir, no se puede manejar".

   El profesional de la seguridad debe ser capaz de medir el estado de los controles de seguridad, el cumplimiento de las propias políticas y la eficacia de los procesos de seguridad. Las clave es tomar algunas métricas de las declaraciones de política de seguridad y medirlas en conjunto, lo que se convierte en un cuadro de mando bien equilibrado para la seguridad.

   El marco de métricas proporciona retroalimentación al marco de procesos con información de las medidas necesarias para ejecutar los procesos de seguridad tal como lo diseñado.

c) Las partes interesadas.

   Las partes interesadas, son los destinatarios de los resultados de las métricas del marco de seguridad. Los interesados tienen que saber que lo que se ha prometido se está entregando. Más importante es la seguridad profesional que mostrar el valor de la seguridad para las empresas. Esta es el área donde los profesionales de la seguridad necesitan mejorar sus habilidades. Hable con sus grupos de interés, pregúnteles ¿cuáles son sus preocupaciones? y muéstreles cómo se están abordando las preocupaciones respecto a su área o ambiente de desarrollo mediante un informe.

2.2.4. El Modelo de Seguridad de la Información en TIC (MSI-TIC).

El modelo considera su estructuración, formación e implementación bajo dos grandes fases:

- Fase de Elaboración
- Fase de Aplicación

Estas fases agrupan un conjunto de actividades, muchas de las cuales llevan a un ciclo continuo de mejora (ver Figura 2.4).

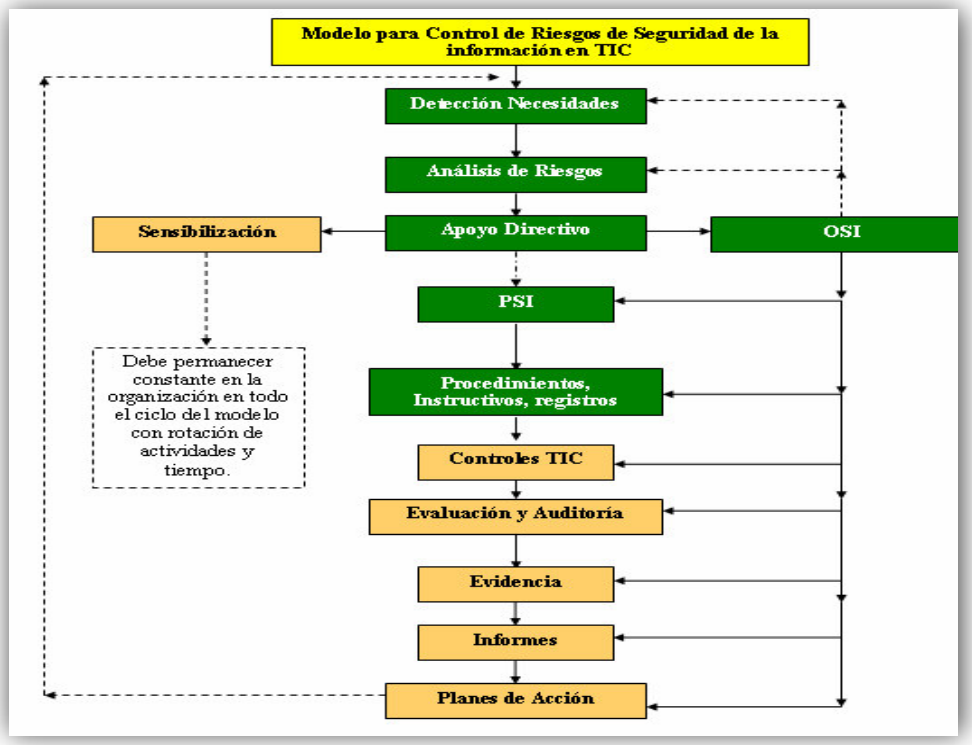


Figura 2.4 Modelo de Seguridad de la información en TIC agrupado por fases y actividades. **[Burgos 2011]**

A continuación se presenta una descripción de las fases y actividades que ellas consideran:

a) Fase de elaboración.

1. Detección de necesidades.

   Corresponde al levantamiento de todas las actividades relacionadas con los impactos que la organización pueda tener en relación con su seguridad de la información.

2. Análisis de riesgo.

   Corresponde a evaluar todos los potenciales riesgos que impactan en la seguridad de la información en los cuales se

pueda ver envuelta la organización por aspectos emanados de las tecnologías de la información.

3. Apoyo directivo.
   Corresponde a la presentación y revisión del resultado de las etapas anteriores con el fin de conseguir de la dirección de la organización el apoyo para concretar la implementación de la seguridad de la información (presupuestos, personal, capacitación, etc.).

4. Oficial de seguridad de la información (OSI).
   La organización debe designar a un OSI para que realice, apoye, dirija y pueda llevar el control de implementación y posterior seguimiento a todo el modelo de seguridad de la información. Además el OSI estará presente en todas las actividades y con énfasis en la fase de aplicación en la cual participa en forma activa en todas las actividades.

5. Confección de política de seguridad de la información (PSI).
   Corresponde al diseño de las Políticas de Seguridad de la Información de la organización.

6. Confección de procedimientos, instructivos y registros.
   Corresponde al desarrollo de documentos que formalicen como se deben realizar las actividades y que información es la que se debe retener como evidencia para dar conformidad a las PSI.

b) Fase de Aplicación.

1. Controles TIC.
   En esta etapa se diseñan y definen los procesos, objetivos de control, controles y evidencias formales de las actividades de seguridad que darán sustento a los procesos de revisión o auditorias del modelo.

2. Evaluación y auditoria.

   En esta etapa se debe realizar, preparar y desarrollar la revisión que avale que todos los procesos de TI se están cumpliendo y llevando a cabo adecuadamente, lo cual será evaluado por el mismo proceso de auditoria (interna y/o externa).

3. Evidencia.

   En esta etapa se busca verificar de manera adecuada que todos los registros de TI para los procesos y controles estén disponibles para cualquier tipo de revisión, particularmente a los procesos de auditoria.

4. Informes.

   Esta etapa contempla la confección de informes del proceso de revisión que derivarán en actividades de mejora al modelo y con revisiones por parte de la dirección de la organización que permitan confeccionar adecuados planes de acción.

5. Planes de Acción.

   Esta etapa consiste en la aplicación de los planes de acción conforme a los plazos y actividades que fueron indicados en el proceso de auditoría. Estos planes de acción pueden conformar la revisión y ajustes de todo tipo de actividades ya sea a nivel de procesos de seguridad, de evidencias, de políticas o de cualquier otra actividad que sea identificada.

6. Sensibilización.

   Esta etapa (incluida en ambas fases del modelo) permite entregar constante información (alertas) a la organización sobre la importancia de mantener la seguridad de la información y el resguardo de todas las actividades de TI. Debe recibir un apoyo directo de la dirección de la organización.

2.2.5. Towards an Information Security Maturity Model for Secure e-Government Services (ISMM).

El modelo propone niveles de madurez con sus respectivas dimensiones de control de seguridad para asegurar los servicios de gobierno electrónico (aplicación y prestación de servicios):

a) Nivel de madurez 1 - No definido.

Este es el nivel de madurez más bajo del modelo de seguridad de la información destinada a las organizaciones con objetivos con baja seguridad de la información en un entorno de seguridad de bajo riesgo, donde las métricas de procesos no son obligatorios. Las políticas de seguridad pueden estar disponibles. Es necesario concientizar a los usuarios de la reducción de riesgos de seguridad frente a las amenazas de seguridad técnicas y no técnicas que pueden ocurrir.

b) Nivel de madurez 2 – Definición.

El segundo nivel de madurez es para las organizaciones con objetivos normales de seguridad de la información en un entorno de riesgos de seguridad normal. Los indicadores de proceso pueden ser usados, pero no es obligatoria. En este nivel, las políticas de seguridad, incluyendo la conciencia, visiones y estrategias son revisadas y actualizadas. Además se realiza la reducción de riesgos de seguridad frente a las amenazas de seguridad técnicas y no técnicas. La seguridad de la información poco a poco se va incrustando en la cultura organizacional.

c) Nivel de madurez 3 – Administrado.

Este es el nivel está dirigido para organizaciones con objetivos rigurosos de seguridad de la información en un entorno de riesgos de seguridad de normal a alta. Se realiza una alta reducción del riesgo de amenazas de seguridad técnicas y no técnicas. En este nivel la métrica de los proceso puede ser utilizada. Además, las políticas de

seguridad, incluyendo la conciencia, visiones y estrategias son regularmente revisados y actualizados.

d) Nivel de madurez 4 – Controlado.

El cuarto nivel de madurez es para organizaciones con objetivos más ambiciosos seguridad de la información en un entorno de riesgos de seguridad alta o superior. Se realiza la más alta reducción de riesgos de seguridad frente a las amenazas de seguridad técnicas y no técnicas. El uso de los indicadores del proceso es obligatorio. La seguridad de la información está incorporada en la cultura de la organización. Además, las políticas de seguridad, conciencia, visiones y estrategias son regularmente revisados y actualizados.

e) Nivel de madurez 5 – Optimizado.

Este se supone que es el más alto nivel de madurez. Está dirigido a organizaciones con objetivos más ambiciosos seguridad de la información en entornos de seguridad de más alto riesgo. Se realiza la más alta reducción de riesgos de seguridad frente a las amenazas de seguridad técnicas y no técnicas. El uso de los indicadores de proceso es obligatorio. Al igual que en el nivel de madurez anterior - las políticas de seguridad, conciencia, visiones y estrategias son regularmente revisados y actualizados. La seguridad de la información está incorporada en la cultura de la organización.

Resumimos los niveles de madurez descritos arriba en una presentación gráfica (ver Figura 2.5), la cual muestra los niveles de madurez del modelo de seguridad de la información, del nivel madurez uno o el más bajo al nivel de madurez cinco o el más alto, donde las cifras sugieren que a medida que se sube a mayores niveles de madurez de seguridad disminuye los riesgos, por consiguiente, se requiere de un mayor esfuerzo para mitigar estos riesgos de seguridad.

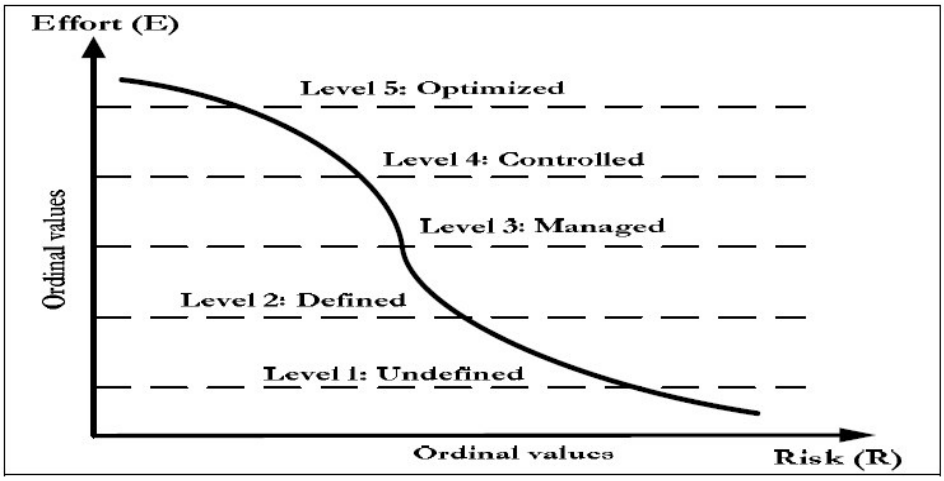


Figura 2.5 ISMM que muestra los niveles de madurez, Riesgos VS Esfuerzos. **[Karokola, 2011]**

Los estudios existentes muestran que más esfuerzos se invierten en el desarrollo de los servicios técnicos de seguridad que en los de seguridad no técnicos. Como resultado, existe una brecha más amplia entre los servicios de seguridad de carácter técnico y no técnico (ver Figura 2.6).

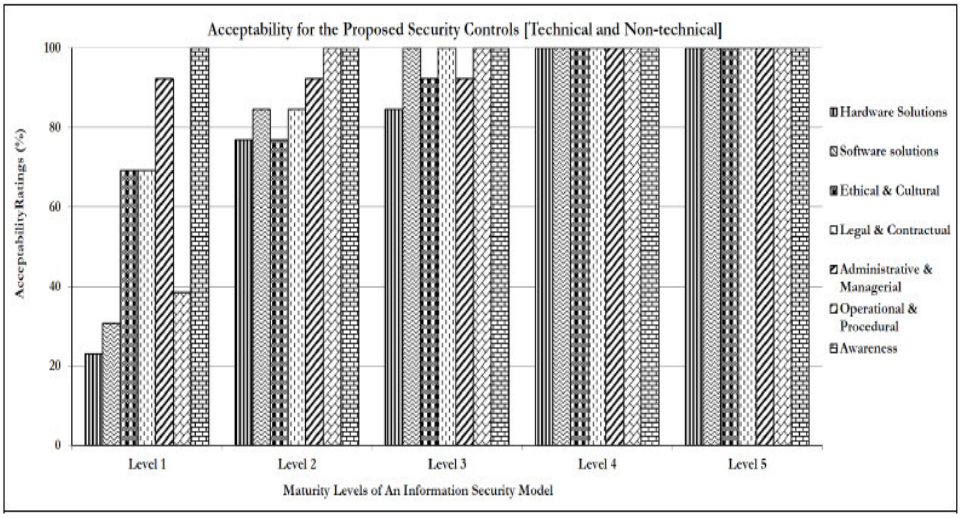


Figura 2.6 Servicios de seguridad por niveles de madurez. **[Karokola, 2011]**

2.2.6. El Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea (MSI-EGL).

El modelo propone una estructura institucional para la estrategia de gobierno en línea (ver Figura 2.7).

Figura 2.7 Estructura institucional del modelo. **[MINTIC, 2011]**

El Modelo de seguridad de la información para las entidades del estado, se apoya en la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en Línea (SASIGEL) y en la conformación de la Comisión de Seguridad de la Información para Gobierno en Línea, para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información en cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de Gobierno en línea.

a) Sistema administrativo de seguridad de la información para gobierno en línea.

   El SASIGEL es el conjunto de todos los actores (públicos, privados y de la sociedad civil) que afectan la seguridad de la información nacional. Asimismo, incorpora el conjunto de las reglas de juego que rigen las interacciones entre todos estos actores.

El SASIGEL coordinará las actividades relacionadas con la formulación, ejecución, seguimiento y mantenimiento de las políticas y lineamientos necesarios para fortalecer la adecuada gestión de seguridad de la información a nivel nacional (ver Figura 2.8).

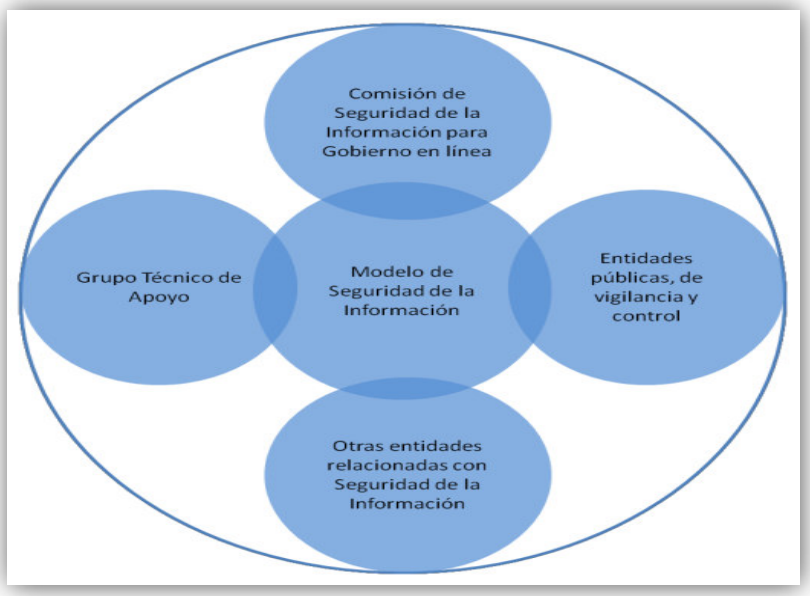


Figura 2.8 Relaciones del SASIGEL. [MINTIC, 2011]

a.1. Comisión de seguridad de la información para gobierno en línea (CSIGEL).

Es el eje central del SASIGEL, es el órgano asesor del Gobierno Nacional y de concertación entre éste, las entidades objetivo e indirectamente con la sociedad civil, en temas relacionados con seguridad de la información del país y de sus territorios para aprobar las políticas en materia de seguridad de información nacional, definir el curso de acciones a seguir y hacer seguimiento para asegurar su cumplimiento y su mantenimiento, con el fin de generar credibilidad y confianza protegiendo la información de las entidades y de los ciudadanos (ver Figura 2.9).

Figura 2.9 Comisión de Seguridad de la Información para Gobierno en línea. **[MINTIC, 2011]**

a.2. El grupo técnico de apoyo.

Su función principal es acotar, dentro de los parámetros establecidos en las normas pertinentes, el modelo de seguridad de la información a nivel táctico y técnico especificando las políticas, objetivos de control y controles propuestos para que sean implementados por cada una de las entidades objetivo.

El grupo técnico de apoyo es el encargado de la preparación de los documentos, políticas, lineamientos, estándares y recomendaciones que son avalados por la comisión. Proporciona apoyo técnico y jurídico a la CSIGEL para la operatividad del modelo, coordina las actividades de capacitación y concientización

b) Equipo de gestión del proyecto del nivel central.

Se encarga de tomar las medidas necesarias para lograr la implementación del modelo de seguridad de la información en las entidades del estado, propender por su adecuada administración y realizar las auditorias necesarias para medir el avance del modelo en las entidades. Además debe analizar, consolidar y publicar los

indicadores, métricas y estadísticas del sistema y del modelo de seguridad implementado en las entidades.

c) Equipo de gestión al interior de cada una de las entidades.
Cada una de las entidades se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el modelo de seguridad de la información al interior de su entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

El Modelo propuesto para la estrategia de gobierno en línea presenta una escala para determinar el nivel (ver Cuadro 2.1) de responsabilidad de la entidad en cuanto a la seguridad de la información, las políticas, objetivos de control y controles recomendados para su implementación y mejoramiento. Las políticas y objetivos de control, dado que son estratégicos y de alto nivel, serán los mismos para todo el universo de entidades independiente del nivel en el que se encuentren; los controles recomendados, si dependerán de la clasificación, es decir, las entidades de acuerdo al puntaje deben cumplir con los controles básicos, medios o avanzados (ver Cuadro 2.1).

Puntos	Clasificación (estrato)
Menor a 11	Bajo
Entre 11 y 22	Medio
Mayor a 22	Alto

Cuadro 2.1 Escala de niveles. **[MINTIC, 2011]**

Presupuesto en Millones de Pesos	Existencia y función del Área de sistemas	No. PC's	No. Servidores	Existencia y Objeto de la WAN	Transaccionalidad en la WEB	Desarrollo de Software	No. Empleados de Sistemas	Puntos que otorga
0 – 2.999	No hay área de sistemas	0 - 99	0 - 3	Internet Solo correo (externo) y navegación	Solo consulta	No. Incluye hosting básico de WEB y correo	0 - 5	**1**
3.000 – 50.000	Soporte Básico día a día y de usuario final. Reactiva	100 - 500	4 - 20	Internet con servicios públicos ofrecidos	Transaccionalidad Local (solo datos propios)	Aplicativos Internos	6 - 50	**2**
>50.000	Área con funciones definidas, administración de presupuesto y desarrollo de proyectos a futuro. Proactiva	>500	>20	Todo lo anterior más WAN privada	Transaccionalidad e interoperabilidad (utiliza datos propios y provee o consulta datos de otras entidades o terceros)	Aplicativos externos (servicios a terceros). Puede o no incluir desarrollos internos	>50	**3**

Cuadro 2.2 Parámetros que se puntúan para determinar el nivel. **[MINTIC, 2011]**

Independiente del nivel y de los controles que las entidades deban aplicar, se debe realizar el seguimiento y control de todos los recursos con el fin de asegurar que los resultados se produzcan oportuna y eficazmente en función de los costos y por otra parte que el alcance definido se cumpla dentro de los tiempos estimados o planeados. Esta labor se debe realizar al interior de las entidades bajo la supervisión y lineamientos del equipo de gestión de nivel central de acuerdo a los indicadores de medición (ver Cuadro 2.3).

INDICADOR DE GESTIÓN EN LA IMPLEMENTACIÓN	METRICA A USAR	FRECUENCIA DE MEDICIÓN
CONTROLES IMPLEMENTADOS	CI = Número de Controles que se planearon instalar / Número de Controles Implementados	Mínimo: Mensual
CONTROLES AJUSTADOS	CA = Número de Controles que se planearon AJUSTAR / Número de Controles Ajustados	Mínimo: Mensual
CONTROLES FUNCIONANDO CORRECTAMENTE	CFC = (Número de Controles instalados + Número de Controles Ajustados) / Número de Controles Funcionando Correctamente	Mínimo: Mensual

Cuadro 2.3 Indicadores y métricas de gestión. **[MINTIC, 2011]**

2.2.7. El Open Information Security Management Maturity Model (O-ISM3).

Es un modelo orientado a procesos que ofrece un enfoque cuantitativo para evaluar la gestión de un sistema de seguridad de la información en una organización, debido a que establece niveles de madurez sobre 04 modelos conceptuales (gestión, organización, sistema de información y seguridad contextual) y la aplicación de métricas para administrar los procesos de seguridad de la información.

La aplicación del O-ISM3 implica la implementación de cada uno de los procesos definidos de acuerdo a las prácticas de gestión de seguridad, el establecimientos de las métricas y el monitoreo del nivel de madurez en que se encuentra dicha implementación.

Asimismo, la gestión de seguridad de la información debe ser reportada desde el nivel operativo hacia los interesados en la organización (ver Figura 2.10).

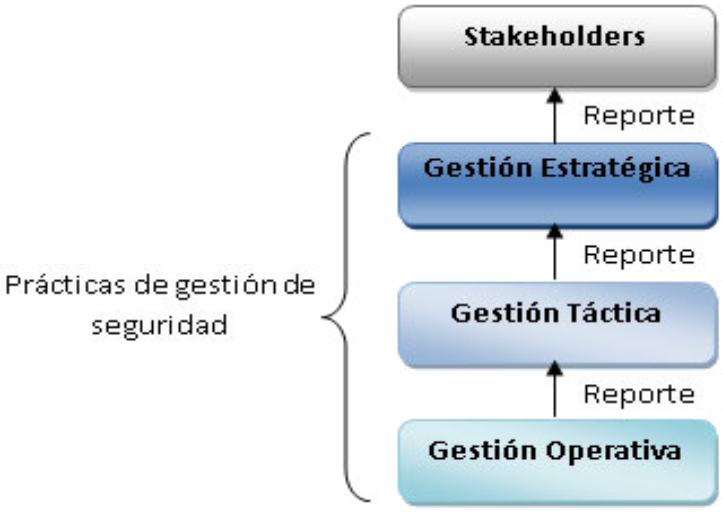


Figura 2.10 Estructura de niveles de reporte de la gestión de seguridad. **[The Open Group, 2011]**

Los procesos establecidos para las prácticas de gestión de seguridad (ver Cuadros 2.4 y 2.5) están compuestos por descripción del proceso,

entradas, productos de trabajo, documentación, propietario del proceso, procesos relacionados y metodologías relacionadas.

Prácticas de gestión	Código	Procesos
Procesos Genéricos	GP-1	Gestión del conocimiento
	GP-2	Auditoría de negocio y del GSI
	GP-3	Diseño y evolución del GSI
Gestión Estratégica	SSP-1	Informar a los accionistas.
	SSP-2	Coordinar.
	SSP-4	Reglas para definir la división de funciones.
	SSP-6	Asignar recursos para seguridad de la información.
Gestión Táctica	TSP-1	TSP-1 Informar a la gestión estratégica.
	TSP-2	Gestionar los recursos asignados.
	TSP-3	Definir las Metas de Seguridad.
	TSP-4	Definir los indicadores para los procesos de seguridad.
	TSP-6	Arquitectura de Seguridad.
	TSP-7	Investigar antecedentes y referencias.
	TSP-8	Seleccionar el personal de seguridad.
	TSP-9	Capacitar al personal de seguridad.
	TSP-10	Definir procesos disciplinarios.
	TSP-11	Alcanzar conciencia en seguridad.
	TSP-13	Gestión de seguros.
	TSP-14	Operaciones de Información.
Gestión Operativa	OSP-1	Informar a la gestión táctica.
	OSP-2	Seleccionar las herramientas para implementar las medidas de seguridad.
	OSP-3	Gestionar el inventario.
	OSP-4	Controlar el cambio del ambiente de los sistemas de información.
	OSP-5	Refaccionar el ambiente.
	OSP-6	Limpiar el ambiente.
	OSP-7	Fortalecer el ambiente.
	OSP-8	Controlar el ciclo de vida del desarrollo de software.
	OSP-9	Controlar los cambios en las medidas de seguridad.
	OSP-10	Gestionar el respaldo y redundancia.
	OSP-11	Controlar el acceso a servicios, canales, repositorios e interfaces.
	OSP-12	Llevar el registro de usuarios.
	OSP-14	Gestionar la protección del ambiente físico.
	OSP-15	Gestionar la continuidad de operaciones.
	OSP-16	Gestionar el filtrado y segmentación.
	OSP-17	Gestionar la protección contra Malware.
	OSP-19	Emular ataques, errores y accidentes.
	OSP-20	Emular incidentes.
	OSP-21	Comprobar la calidad de la información.
	OSP-22	Monitorizar alertas.
	OSP-23	Detección y Análisis de eventos internos.

	OSP-24	Manejar los incidentes y pseudo-incidentes.
	OSP-25	Realizar el análisis forense.
	OSP-26	Gestión de una mejor fiabilidad y disponibilidad
	OSP-27	Gestión de archivo
	OSP-28	Detección y Análisis de eventos externos.

Cuadro 2.4 Relación de procesos por nivel organizacional. **[The Open Group, 2011]**

	Niveles				
Procesos evaluados	0 Inicial	1 Administrado	2 Definido	3 Controlado	4 Optimizado
Procesos Genéricos	3	3	3	3	3
Gestión Estratégica	3	3	3	4	4
Gestión Táctica	3	6	8	10	12
Gestión Operativa	5	14	18	23	26

Cuadro 2.5 Procesos revisados por nivel de madurez. **[The Open Group, 2011]**

Finalmente se muestra las métricas necesarias para los procesos en cada nivel (ver Cuadro 2.6).

Nivel		Inicial	Administrado	Definido			Controlado	Optimizado
Prácticas de gestión		Certificación de auditoría	prueba	Monitorizar	Planificación	Realización de beneficios	Valorización	Optimización
Tipo de métrica	Documentación	X	X	X	X	X	X	X
	Actividad		X	X	X	X	X	X
	alcance		X	X	X	X	X	X
	falta de disponibilidad		X	X	X	X	X	X
	eficiencia		X	X	X	X	X	X
	Carga			X	X	X	X	X
	calidad						X	X
	eficacia							X

Cuadro 2.6 Métricas por nivel de madurez. **[The Open Group, 2011]**

2.2.8. El Modelo Contextualizado de Colado & Franco (MCC&F).

El modelo basa las métricas en la triangulación de condiciones de seguridad informática (ver Figura 2.11).

Condicionales para la triangulación

- ¿Para qué? se refiere a la indagación del estado de la seguridad informática en la organización.
- ¿Qué? se refiere a las fuentes de información utilizadas y se destacan la revisión bibliográfica, el cuestionario y las entrevistas.
- ¿Cómo? tiene que ver con el análisis de los datos obtenidos en las fuentes de información.

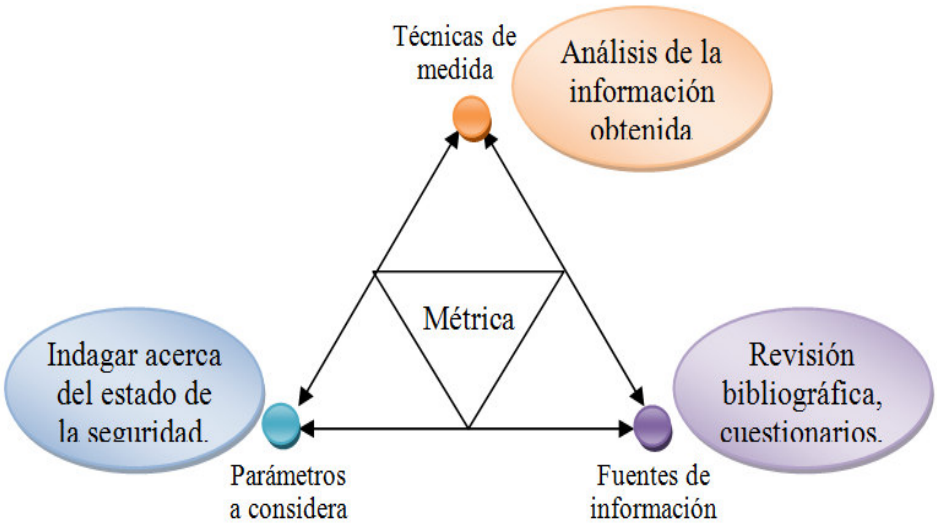


Figura 2.11 Contextualización de la seguridad. **[Villegas, 2011]**

El resultado de la aplicación del modelo contextualizado permita identificar y establecer los principales indicadores para la gestión de la seguridad y agruparlos en los 4 niveles establecidos (ver Cuadro 2.7) con la finalidad de poder medir el desempeño institucional frente a los retos que plantea la preservación y resguardo informático.

Niveles	Descripción
Estado inicial de seguridad informática	Etapa inicial en la que se hace el diagnóstico del estado de seguridad de las universidades estudiadas.
Detección de necesidades	Etapa en la que se describen e identifican los elementos necesarios para mejorar la seguridad informática.
Planificación estratégica	Etapa en la que se realiza trabajo en equipo para afinar el diagnóstico, establecer un plan estratégico para crear políticas de seguridad informática.
Inteligencia organizacional	Etapa en la que aplica el plan estratégico y se hacen correcciones sobre la marcha para optimizar la seguridad informática.

Cuadro 2.7 Niveles de medición del desempeño. **[Villegas, 2011]**

2.2.9. ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información (SGSI).

Este modelo es considerado un estándar internacional que ha sido elaborado para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la Gestión de Seguridad de la Información en las organizaciones. La adopción del SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

Este estándar internacional promueve la adopción de un enfoque de proceso, lo cual fomenta que sus usuarios enfaticen la importancia de:

a) Entender los requerimientos de seguridad de la información de una organización y las expectativas de las partes interesadas, así como la necesidad de establecer una política y objetivos para la seguridad de la información;

b) Implementar y operar controles para manejar los riesgos de seguridad de la información;
c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
d) Mejoramiento continuo en base a la medición del objetivo.

El modelo del proceso adoptado es el de Planear-Hacer-Chequear-Actuar (PDCA), el cual se aplica a todos los procesos SGSI (ver Figura 2.12).

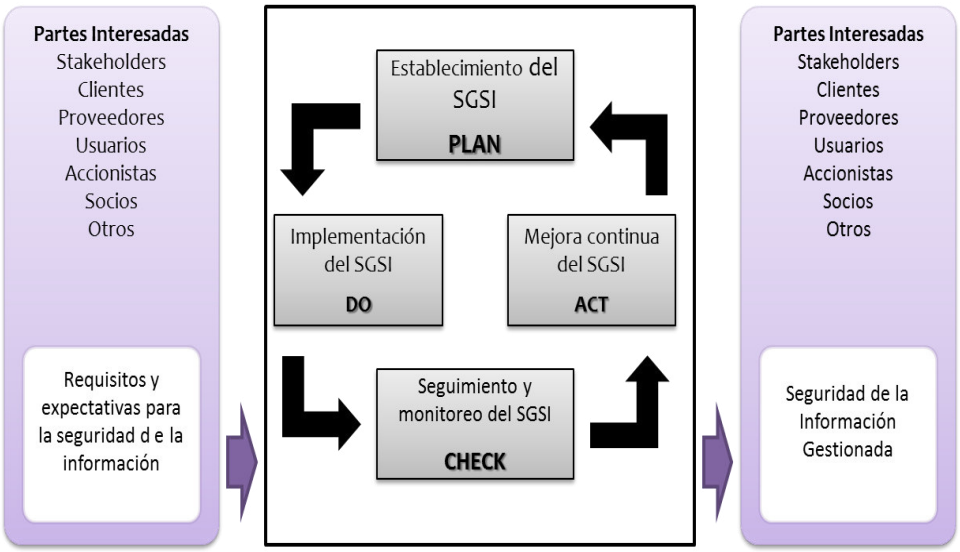


Figura 2.12 Modelo PDCA aplicado a los procesos del SGSI. **[ISO, 2013]**

La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan, de acuerdo a los requisitos definidos en los capítulos del 4 al 10 (ver Figura 2.13) y de los objetivos de control y controles del anexo A del estándar (ver Cuadro 2.8).

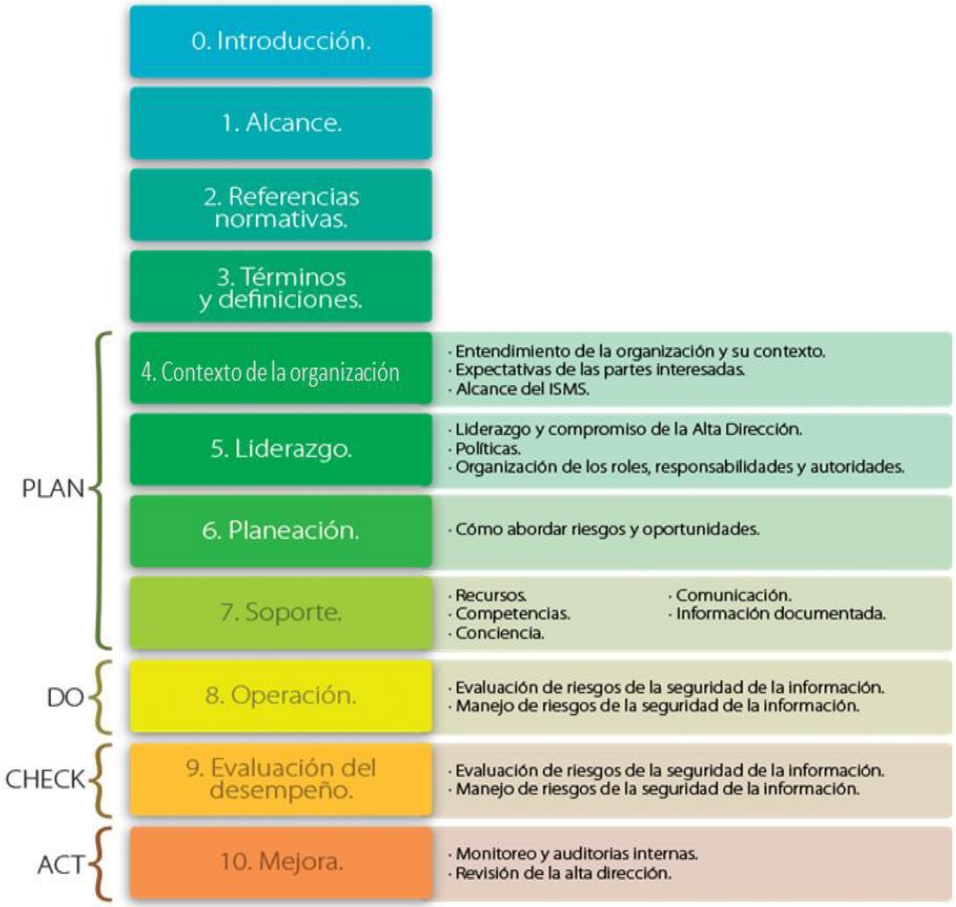


***Figura 2.13 Cláusulas definidas en el estándar de acuerdo al modelo PDCA*. [ISO, 2013]**

Cláusula	Sec.	Objetivo de Control	Control
Políticas de seguridad de la información.	5.1	Dirección de la gerencia para la seguridad de la información.	2
Organización de la seguridad de la información.	6.1	Organización Interna.	5
	6.2	Dispositivos móviles y teletrabajo.	2
Seguridad de los recursos humanos.	7.1	Antes del empleo.	2
	7.2	Durante el empleo.	3
	7.3	Terminación y cambio de empleo.	1
Gestión de activos.	8.1	Responsabilidad por los activos.	4
	8.2	Clasificación de la información.	3
	8.3	Manejo de los medios.	3
Control de acceso.	9.1	Requisitos de la empresa para el control de acceso.	2
	9.2	Gestión de acceso de usuario.	6
	9.3	Responsabilidades de los usuarios.	1
	9.4	Control de accesos a sistemas y aplicaciones.	5

Cláusula	Sec.	Objetivo de Control	Control
Criptografía.	10.1	Controles criptográficos.	2
Seguridad física y ambiental.	11.1	Áreas seguras.	6
	11.2	Equipamiento.	9
Seguridad de las operaciones.	12.1	Procedimientos y responsabilidades operativas.	4
	12.2	Protección de malware.	1
	12.3	Respaldo.	1
	12.4	Bitácoras y monitoreo.	4
	12.5	Control del software operacional.	1
	12.6	Gestión de vulnerabilidad técnica.	2
	12.7	Consideraciones para la auditoría de los Sistemas de información.	1
Seguridad de las comunicaciones.	13.1	Reporte de eventos de seguridad informática y de sus debilidades.	3
	13.2	Transferencia de información.	4
Adquisición, desarrollo y mantenimiento del sistema.	14.1	Requisitos de seguridad de los sistemas de información.	3
	14.2	Seguridad en los procesos de desarrollo y soporte.	9
	14.3	Datos de prueba.	1
Relaciones con los proveedores.	15.1	Información de seguridad en las relaciones con los proveedores.	3
	15.2	Gestión de entrega de servicios del proveedor.	2
Gestión de incidentes de seguridad de la información.	16.1	Gestión de incidentes y mejoras a la seguridad de la información.	7
Seguridad de la información en torno a la gestión de continuidad del negocio.	17.1	Continuidad de seguridad de la información.	3
	17.2	Redundancias.	1
Cumplimiento.	18.1	Cumplimiento con requisitos legales y contractuales.	5
	18.2	Revisiones de seguridad de la información.	3

Cuadro 2.8 Objetivos de control y controles del anexo A de la ISO 27001:2013. **[ISO, 2013]**

2.2.10. Directiva de Seguridad de Seguridad de la Información para la Protección de Datos Personales (DSI-PDP)

Orienta la adopción de medidas de seguridad de la información, específicamente para la protección de los bancos de datos personales, para lo cual propone responsabilidades, requisitos de seguridad y establece medidas específicas de seguridad organizativas, jurídicas y técnicas de para asegurar la confidencialidad, disponibilidad e integridad de la información.

La adopción de las medidas de seguridad se debe realizar de acuerdo a la categorización establecida (Básico, Simple, Intermedio, Complejo, Crítico) según el tipo, tiempo de tratamiento y tamaño de la información (ver Figura 2.14). Asimismo para el caso de la información categorizada como crítica se indica que esta debe ser parte del alcance de un Sistema de Gestión de Seguridad de la Información.

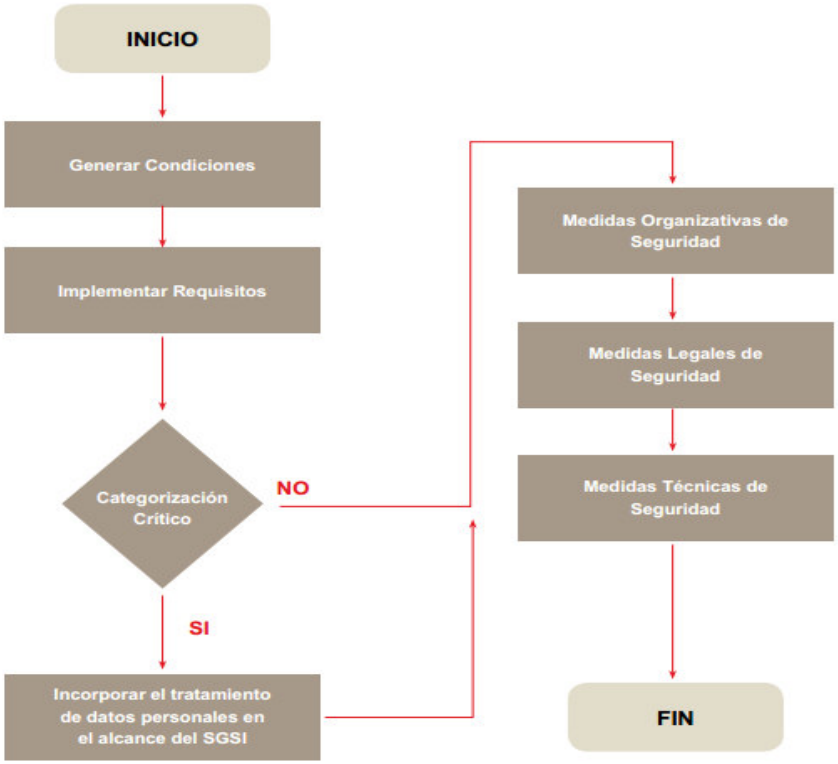


Figura 2.14 Flujo para la aplicación de medidas de seguridad. **[APDP, 2013]**

2.2.11. La Guía Metodológica del Sistema de Seguridad de la Información en el Programa de Mejoramiento de la Gestión y Metas de Eficiencia Institucional (SSI-PMGMEI).

La guía plantea un modelo de seguridad de la información que permite ir conformando un marco de gobierno para la seguridad de la información institucional, al establecer políticas, procedimientos y controles en relación a los objetivos estratégicos de la institución, con objeto de mantener siempre el riesgo por debajo del nivel aceptable por la propia organización.

El modelo plantea un esquema para su implantación y operación dividido en 04 etapas (ver Figura 2.15), asimismo establece una relación de actividades detalladas para el desarrollo de cada uno de los requisitos y controles de seguridad (ver Cuadro 2.9) y una propuesta de indicadores de desempeño que permitan medir la efectividad del sistema de seguridad de la información.

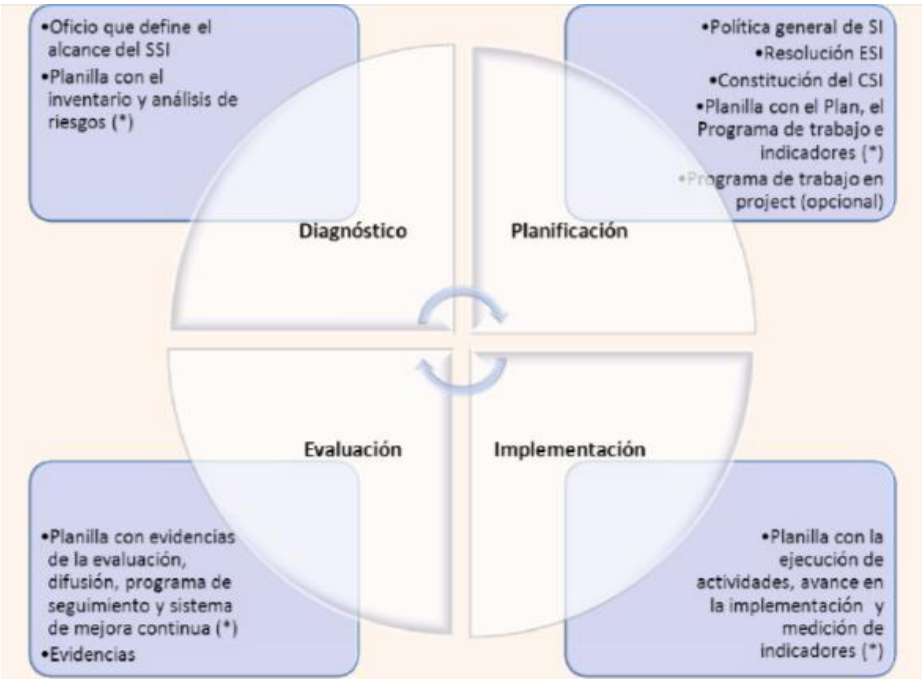


Figura 2.15 Cláusulas definidas en el estándar de acuerdo al modelo PDCA. **[DIPRES, 2014]**

Etapas	Principales actividades
a) Diagnóstico	• Identificar de los activos de información. • Realizar la evaluación de riesgos. • Identificar controles.
b) Planificación	• Establecer de un marco general (política, encargado de seguridad y comité de seguridad de la información) • Elaborar un plan general y programa de trabajo. • Establecer indicadores para medir la efectividad.
c) Implementación	• Ejecutar de las actividades planificadas. • Medir de indicadores.
d) Evaluación	• Evaluar de la implementación del plan general. • Difundir los resultados. • Programar el seguimiento de las recomendaciones. • Mantener el grado de desarrollo alcanzado.

Cuadro 2.9 Principales actividades por etapa. **[DIPRES, 2014]**

2.3. Evaluación comparativa.

De los 11 modelos de seguridad de la información analizados (ver Cuadro 2.10) se concluye que estos contemplan los elementos siguientes:

- *Fases* para implementar, operar, monitorear y mejorar la seguridad de la información.
- *Organización* para la operación de seguridad de la información.
- *Funciones* definidas del responsable o de la dirección de la gestión.
- *Niveles de madurez* del sistema de seguridad.
- *Documentos* obligatorios de seguridad de la información.
- *Controles* definidos para reducir los riesgos de seguridad de información.
- *Indicadores* para medir los controles.
- *Métricas* para determinar el valor de los indicadores de control.

Elementos	Modelos de Seguridad de la Información											Total de modelos por elemento
	MOSSIU	MMASI	GRC	MSI - TIC	ISMM	MSIEGL	O-ISM3	MCC&F	SGSI	DSI - PDP	SSI - PMGMEI	
Fases	04 componentes relacionados	No	03 componentes	fases de Elaboración y Aplicación.	No	04 - PDCA	04- Pirámide administrativa y Proceso general	03 componentes relacionados	04 - PDCA	No	04 diagnostico, planificación implementación y evaluación	8
Organización	No	No	No	No	No	Determinada por la entidad	No	No	Determinada por la entidad	Determinada por la entidad	Determinada por la entidad	4
Funciones	No	No	No	Del Oficial de Seguridad	No	Determinada por la entidad	No	No	No	Requisitos organizativos	No	3
Documento	No	No	Mención en componente conductor	Mención general	No	Mención general	Generales	No	Generales	Requisitos jurídicos	Generales	7
Niveles	No	05	No	No	05	No	05	04	No	No	No	4
Controles	No	No	No	Mención general	No	De acuerdo a clasificación	Especifica por fases	No	Requisitos específicos	Requisitos Técnicos	Mención general	6
Indicadores	No	Mención en cada nivel	No	No	No	Mención general	Mención de 8 tipos	No	No	No	No	3
Métricas	No	No	No	No	No	No	Mención general	Mención general	No	No	No	2

Cuadro 2.10 comparación de los modelos de acuerdo a los elementos identificados.

Asimismo, se puede observar que los modelos en su mayoría se han enfocado principalmente en las fases (08 modelos), documentación (07 modelos) y controles (06 modelos), existiendo poca relevancia en lo correspondiente a organización, funciones, niveles, indicadores y métricas (ver Cuadro 2.11).

Elementos	Número de Modelos por elemento	% de Modelos por elemento
1. Fases	8	73%
2. Organización	4	36%
3. Funciones	3	27%
4. Documento	7	64%
5. Niveles	4	36%
6. Controles	6	55%
7. Indicadores	3	27%
8. Métricas	2	18%

Cuadro 2.11 Relación de elementos identificados por modelo.

3 CAPITULO III: APORTE

Si bien los modelos de seguridad de la información han dado solución a problemas específicos basados en las buenas prácticas del desarrollo empresarial, se observa que son modelos genéricos que tienen que adaptarse a la realidad y problemática de las instituciones y de cada país; como es el caso de la seguridad de la información para el gobierno electrónico, los modelos de seguridad no son claros en cuanto a la organización que gestiona la seguridad de la información, las funciones de sus responsables y no cuentan con indicadores y métricas que permitan determinar el nivel de madurez de seguridad de la información.

En ese contexto, es necesario un modelo que sea claro y apoye a la gestión de la seguridad de la información en los servicios del gobierno electrónico de acuerdo a su fase de desarrollo, tanto a nivel entidad como a nivel país.

El gobierno electrónico puede ser visto a través de cuatro tipos de servicios

- Gobierno a Ciudadano (G2C)
- Gobierno a Empresa (G2B)
- Gobierno a Empleado (G2E)
- Gobierno a Gobierno (G2G)

Asimismo, se cuenta con fases de desarrollo de los servicios de gobierno electrónico:

- Presencia: fase en la que los gobiernos ponen en línea información básica sobre leyes, reglamentos, documentos y estructuras organizacionales, sin mayor relación con los ciudadanos.

- Interacción: fase en la que se generan las primeras interacciones entre ciudadanos y empresas con el gobierno. Se involucran los procesos gubernamentales mediante su mejoramiento y simplificación, abriendo ciertos canales de comunicación para los ciudadanos, empresas y propio gobierno.
- Transacción: fase en la que se permite completar trámites y el pago de tasas e impuestos mediante la implementación del medio de pago virtual (tarjetas de crédito o débito), mejorando la productividad y la participación de los ciudadanos.
- Transformación: fase en la que cambian las relaciones entre el gobernante y el ciudadano. Se realizan cambios en la forma de operar del gobierno y los beneficios originados son recibidos y utilizados, en gran medida por los ciudadanos y empresas.

En el presente capítulo se describe de manera general y específica el Modelo de Gestión de Seguridad de Información para el Gobierno Electrónico (MGSI-EGob) y todos sus elementos, obtenido de los modelos de seguridad de la información revisados en el capítulo 2, cuyo resultado es base para la motivación.

3.1. Modelo Conceptual

Del análisis y evaluación comparativa de los modelos realizada en el capítulo 2, se ha seleccionado aquellos que describen de manera más detallada los elementos que conformarán el modelo (ver Figuras 3.1 y 3.2). Asimismo se ha definido las actividades a realizar para cada uno de los elementos de acuerdo al nivel de madurez (ver Cuadro 3.1), puntualizando la documentación de gestión a elaborar por nivel (ver Cuadro 3.2) y los controles que deben ser documentados (ver Cuadro 3.3).

Figura 3.1 Selección de elementos por modelo estudiado.

Figura 3.2 Modelo conceptual del MGSI-EGob.

Elementos	Detalle por niveles de madurez				
1. Niveles	**Inicial**	**Gestionado**	**Definido**	**Controlado**	**Optimizado**
2. Fases	Plan	Plan / Do	Plan / Do	Plan / Do / Check	Plan / Do / Check / Act
3. Organización	Alta dirección designa responsable de SI.	Alta dirección designa responsable de SI.	Alta dirección designa responsable de SI.	Organización a nivel Estratégica, táctica y operativa	Organización a nivel Estratégica, táctica y operativa
4. Funciones	Definida del responsable de SI.	Definida del responsable de SI.	Definida del responsable de SI.	Definida para cada nivel	Definida para cada nivel
5. Documento	10	10	10	10	10
6. Controles	30	91	107	114	114
7. Indicadores	-	-	4	5	6
8. Métricas	-	-	Por tipo de indicador	Por tipo de indicador	Por tipo de indicador

Cuadro 3.1 Detalle de elementos por niveles de madurez.

Documentos del Modelo GSI-EGob
1. Alcance del SGSI
2. Políticas y objetivos de seguridad de la información
3. Metodología de evaluación y tratamiento de riesgos
4. Declaración de aplicabilidad
5. Plan de tratamiento del riesgo
6. Informe sobre evaluación y tratamiento de riesgos
7. Procedimiento para control de documentos
8. Controles para gestión de registros
9. Procedimiento para auditoría interna
10. Procedimiento para medidas correctivas

Cuadro 3.2 Documentos a elaborar por nivel.

Controles documentados	Documentos				
	Inicial	Gestionado	Definido	Controlado	Optimizado
1. Definición de funciones y responsabilidades de seguridad				X	X
2. Inventario de activos			X	X	X
3. Uso aceptable de los activos		X	X	X	X
4. Política de control de acceso		X	X	X	X
5. Procedimientos operativos para gestión de TI	X	X	X	X	X
6. Acuerdo de confidencialidad	X	X	X	X	X
7. Principios de ingeniería para sistema seguro		X	X	X	X
8. Política de seguridad para proveedores		X	X	X	X
9. Procedimiento para gestión de incidentes	X	X	X	X	X
10. Procedimientos de la continuidad del negocio			X	X	X
11. Requisitos legales, normativos y contractuales	X	X	X	X	X
12. Política Trae tu propio dispositivo (BYOD)	X	X	X	X	X
13. Política sobre dispositivos móviles y tele-trabajo	X	X	X	X	X
14. Política de clasificación de la información		X	X	X	X
15. Política de claves		X	X	X	X
16. Política de eliminación y destrucción		X	X	X	X
17. Procedimiento para trabajo en áreas seguras		X	X	X	X
18. Política de pantalla y escritorio limpio		X	X	X	X
19. Política de gestión de cambio		X	X	X	X
20. Política de creación de copias de seguridad	X	X	X	X	X
21. Política de transferencia de la información	X	X	X	X	X
22. Análisis del impacto en el negocio			X	X	X
23. Plan de prueba y verificación			X	X	X
24. Plan de mantenimiento y revisión			X	X	X

Cuadro 3.3 Controles documentados a elaborar por nivel.

3.2. Modelo de Gestión de Seguridad de la Información para el E-Gobierno (MGSI-Egob)

Como resultado del análisis realizado en la revisión de la literatura, se propone el Modelo de Gestión de Seguridad de la Información para el E-Gobierno, el cual se basa en un enfoque de procesos, teniendo como entradas los requisitos y expectativas de seguridad de la información que requiere la entidad en cuanto a sus servicios de gobierno electrónico, para ser atendidos por el modelo y obtener como salidas dichos servicios acorde a los requisitos y expectativas; el modelo contempla los 08 elementos identificados (ver Figura 3.3).

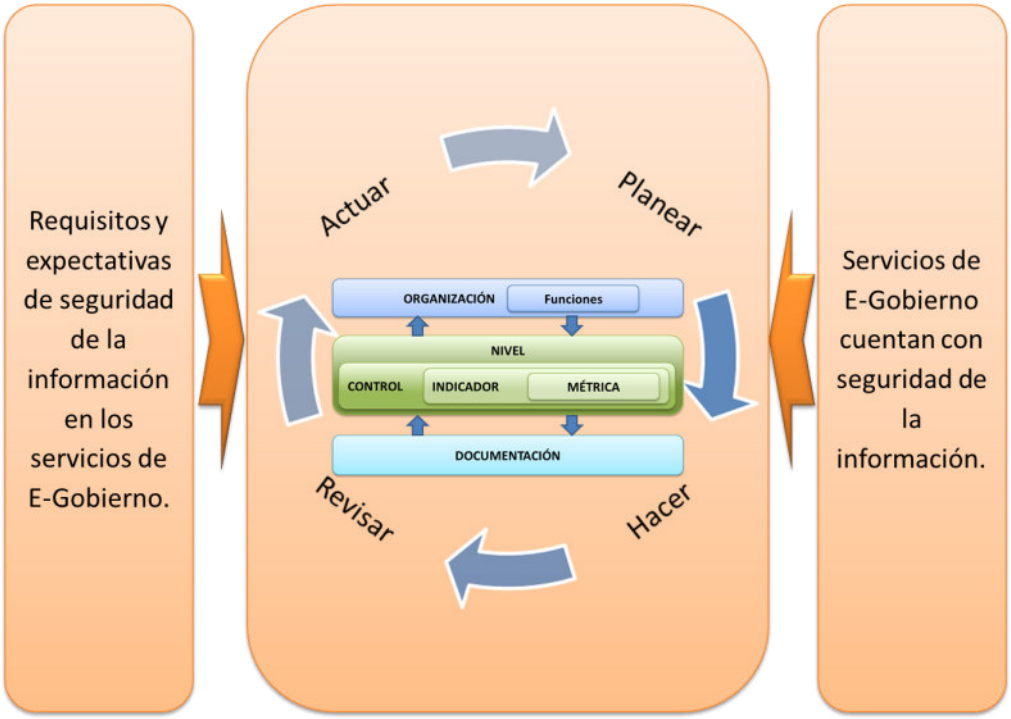


Figura 3.3 Modelo de Gestión de Seguridad de la Información para el E-Gobierno.

3.3. Guía de Implementación del Modelo de Gestión de Seguridad de la Información para el Gobierno Electrónico.

La guía de implementación orienta en el desarrollo del modelo propuesto a fin de gestionar la seguridad de la información en las operaciones referidas al gobierno electrónico de manera eficiente y eficaz.

El desarrollo de la presente guía se realiza de acuerdo a la organización y fases establecidas, las cuales contemplan una serie de actividades, tal como se detallan a continuación:

3.3.1. Fases

El modelo comprende las fases del ciclo de Deming (planear, hacer, revisar y actuar), lo cual permitirá la mejora continua de la seguridad de la información de los servicios de gobierno electrónico brindados por la entidad, teniendo como entrada del proceso los objetivos estratégicos de la organización, los requisitos y expectativas de seguridad de la información y servicios de e-gobierno, las leyes y regulaciones relacionadas al e-gobierno y seguridad de la información; y como las salidas son los controles de seguridad implementados en los servicios de gobierno electrónico, conformidad de riesgos y cumplimiento de las leyes y regulaciones, nivel de desempeños de la gestión de seguridad de la información y los riesgos aceptados (ver Figura 3.4).

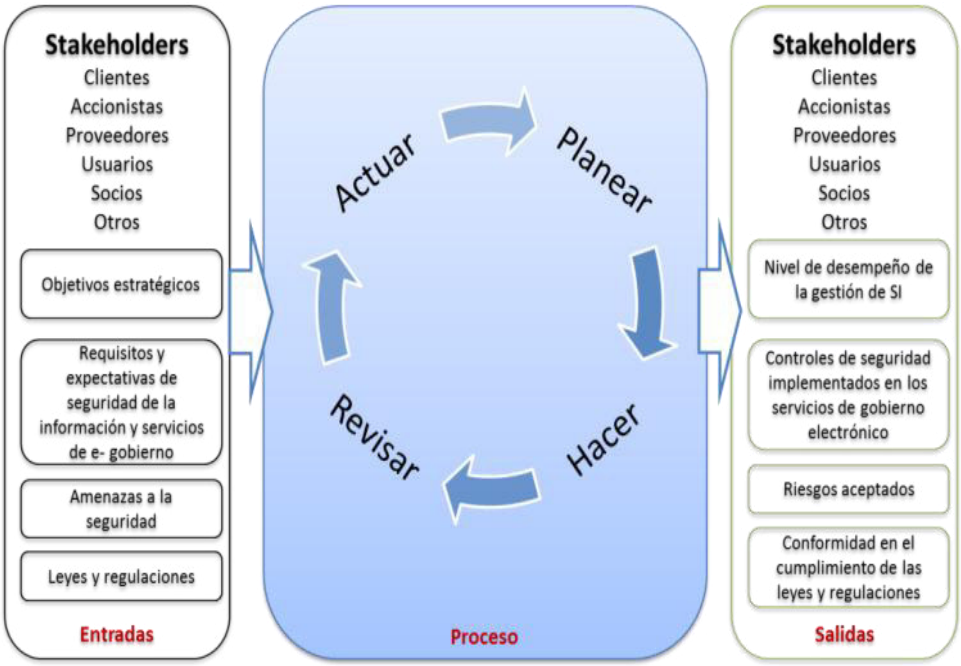


Figura 3.4 Fases del Modelo de Gestión de Seguridad de la Información para el E-Gobierno.

3.3.1.1.Planear

En esta fase la entidad debe:

- Determinar la *política* y *objetivos* de seguridad de la información.
- Determinar el *alcance* de acuerdo a las fases de desarrollo de los servicios de gobierno electrónico brindado por la entidad.
- Establecer el modelo de análisis de evaluación de riesgos.
- Realizar la evaluación de riesgos.
- Elaborar un plan de actividades de los controles a implementar.
- Coordinar la asignación de los recursos necesarios para el plan de actividades.

3.3.1.2.Hacer

En esta fase la entidad debe:

- Sensibilizar al personal sobre las medidas de seguridad implementadas
- Ejecutar el plan de actividades de los controles a implementar.
- Elaborar la documentación del SGSI.
- Definir los indicadores y métricas de los controles a implementar
- Utilizar los recursos necesarios para la ejecución del plan de actividades.

3.3.1.3.Revisar

En esta fase la entidad debe:

- Revisar el cumplimento de los objetivos de seguridad de la información.
- Revisar la eficacia de los controles implementados

- Identificar las causas de las brechas de seguridad de la información
- Elaborar un plan de medidas correctivas.
- Mantener o ampliar el alcance del MGSI-EGob.

3.3.1.4. Actuar

En esta fase la entidad debe:

- Implementar las medidas correctivas.
- Ajustar los indicadores y métricas de los controles modificados o cambiados.

3.3.2. Organización

La entidad debe establecer formalmente la estructura organizacional que gestionará el Sistema de Seguridad de la Información, la cual debe contemplar los procesos estratégicos, fundamentales y de soporte (ver figura 3.5)

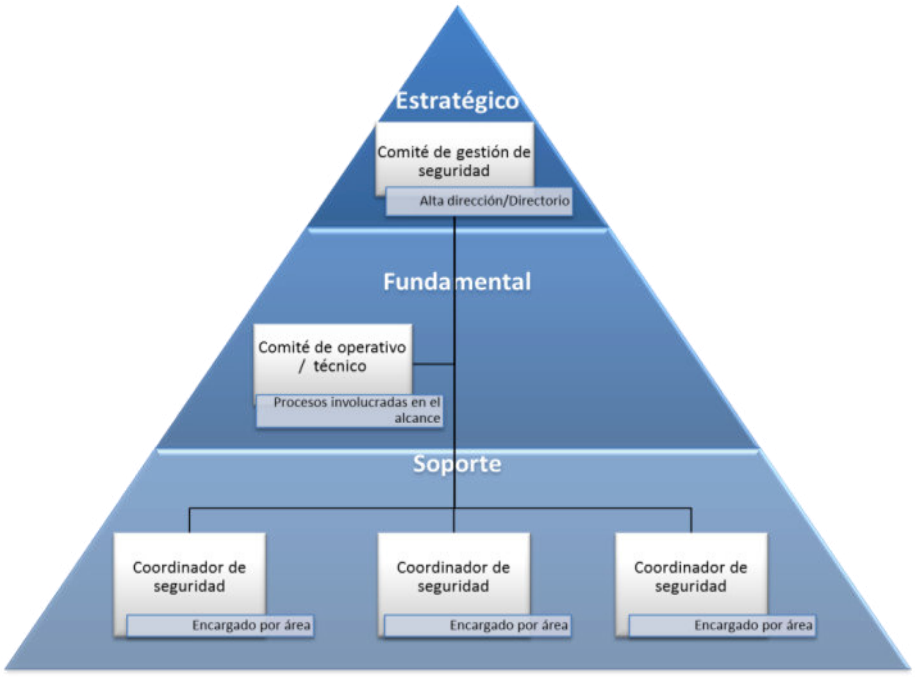


Figura 3.5 Organización del Modelo de Gestión de Seguridad de la Información para el E-Gobierno.

- El Comité de Gestión de Seguridad, debe estar conformado por la alta dirección o por los responsables de los procesos del nivel estratégico.
- El Comité Operativo o Técnico, debe estar conformado por personal representante de los procesos del nivel fundamental que formen parte del alcance del MGSI-EGob o por el área encargada de la seguridad de la entidad.
- Coordinadores de Seguridad de la Información, deben ser los representantes de los sub procesos o áreas de los procesos involucrados en el alcance del MGSI-EGob y de los procesos del nivel soporte.

3.3.3. Funciones

La entidad debe establecer las funciones para los representantes de la organización definida, tal como se detallan a continuación:

a) Comité de Gestión de Seguridad.

   Conformado por la alta dirección, directorio o principales stakeholders, quienes tienen las siguientes funciones:

   - Establecer los lineamientos y directrices del MGSI-EGob.
   - Definir y aprobar la política, objetivos y alcance del MGSI-EGob.
   - Aprobar las normativas o directivas.
   - Gestionar los recursos para la implementación y operación.
   - Designar al comité operativo.
   - Designar responsables para las actividades de implementación.
   - Gestionar el sistema de seguridad de la información planteado por el MGSI-EGob.
   - Monitorear la implementación y operación del MGSI-EGob.

b) Comité de Operativo o Técnico.

Conformado por los encargados de las áreas involucradas en el proceso del MMGSI-eGob, quienes tienen las siguientes funciones:

- Realizar el análisis y evaluación de riesgos.
- Elaborar un plan de tratamiento de riesgos.
- Implementar los controles del MGSI-EGob.
- Evaluar periódicamente la implementación y operación del modelo.
- Definir indicadores y métricas de los controles.
- Elaborar y difusión de políticas, normativas o directivas de seguridad o documentación necesaria para el MGSI-EGob.
- Determinar las acciones preventivas y correctivas.

c) Coordinadores de Seguridad de la Información.

Personal designado en una U.O, área o proceso, quienes tienen las siguientes funciones:

- Desarrollo y seguimiento de controles bajo su ámbito.
- Tomar acciones inmediatas.
- Evaluar la eficacia de los controles bajo su ámbito.
- Informar sobre los incidentes de seguridad al comité operativo.
- Reportar periódicamente la situación de la seguridad de la información.

3.3.4. Documentos

La entidad debe contar con la documentación del Sistema de Gestión de Seguridad de la información; dicha información debe ser revisada, aprobada, almacenada y controlada.

Los documentos obligatorios a elaborar son:

1. Alcance del SGSI.
2. Políticas y objetivos de seguridad de la información.
3. Metodología de evaluación y tratamiento de riesgos.

4. Declaración de aplicabilidad.
5. Plan de tratamiento del riesgo.
6. Informe sobre evaluación y tratamiento de riesgos.
7. Procedimiento para control de documentos.
8. Controles para gestión de registros.
9. Procedimiento para auditoría interna.
10. Procedimiento para medidas correctivas.

3.3.5. Niveles

En el modelo se han definido niveles de madurez de acuerdo a los servicios que brinda el gobierno electrónico y la fase de desarrollo con que cuenta un determinado servicio (ver Figura 3.6).

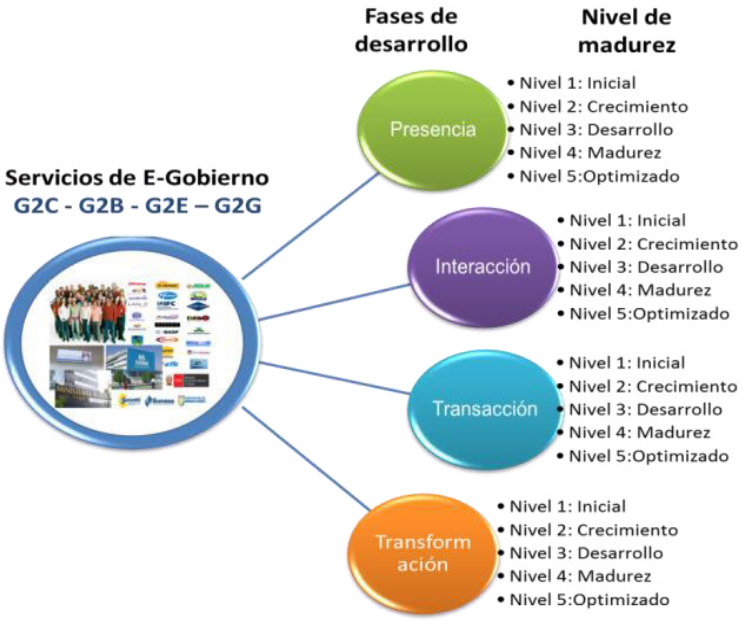


Figura 3.6 Niveles de madurez de acuerdo a las fases de desarrollo del servicio de E-Gobierno.

Para determinar el nivel de madurez se debe considerar lo siguiente:

- Cumplir con lo requerido de acuerdo a cada nivel de madurez, tal como se detalló en el cuadro 3.1.
- Gestionar la documentación detallada en el cuadro 3.2.

- Implementar los controles detallados en el cuadro 3.3, se pueden excluir aquellos controles propuestos para actividades que la entidad no realiza o no afectan la continuidad de sus operaciones.
- Evaluar el nivel de cumplimiento de la documentación y controles.

Se ha establecido una escala de evaluación del 0 al 5, en la que para la aceptación de cumplimiento de los niveles de inicial a definido el valor mínimo de la evaluación deberá ser 3, para el nivel controlado deberá ser 4 y par el nivel optimizado deberá ser 5 (ver Cuadro 3.4).

Calificación	Efectividad	Cumplimiento con respecto al control: es un control débil, cumple o excede las expectativas.
0	**0%**	No se definido ningún tipo de control
1	**10%**	No existen controles efectivos – deficiencias considerables con respecto a lo esperado para el requerimiento.
2	**50%**	Controles Básicos – deficiencias menores con respecto a lo esperado para el requerimiento.
3	**80%**	El requerimiento cuenta con indicadores y se cumple en forma efectiva.
4	**95%**	El requerimiento cuenta con indicadores y registros.
5	**100%**	El requerimiento cuenta con indicadores y registros monitoreados.

Cuadro 3.4 Escala de evaluación de controles.

3.3.6. Controles

Son las actividades que se realizan para tratar los riesgos de seguridad de la información que afecten el logro de los objetivos de la entidad.

Para cada nivel de interacción del servicio se deben implementar controles que ayuden a determinar el nivel de madurez en que se encuentra el Sistema de Gestión de Seguridad de la Información, dichos controles se han obtenido de la combinación de controles propuestos por

el estándar ISO 27001 e ISM3 para cada nivel de madurez (ver Cuadro 3.5).

ISO 27001	ISM3	Nivel 1: inicial	Nivel 2: Crecimiento	Nivel 3: Desarrollo	Nivel 4: Madurez	Nivel 5: Optimizado
5.1.1	GP-1	X	X	X	X	X
5.1.2	GP-1	X	X	X	X	X
6.1.1	GP-3	X	X	X	X	X
6.1.2	SSP-4				X	X
6.1.3	SSP-2	X	X	X	X	X
6.1.4	SSP-2	X	X	X	X	X
6.1.5	TSP-6		X	X	X	X
6.2.1	OSP-16	X	X	X	X	X
6.2.2	OSP-16	X	X	X	X	X
7.1.1	TSP-7				X	X
7.1.2	TSP-8				X	X
7.2.1	TSP-8				X	X
7.2.2	TSP-11		X	X	X	X
7.2.3	TSP-10		X	X	X	X
7.3.1	OSP-12		X	X	X	X
8.1.1	OSP-3			X	X	X
8.1.2	OSP-3			X	X	X
8.1.3	OSP-4		X	X	X	X
8.1.4	OSP-4		X	X	X	X
8.2.1	OSP-3		X	X	X	X
8.2.2	OSP-3		X	X	X	X
8.2.3	OSP-3 / OSP-4		X	X	X	X
8.3.1	OSP-4		X	X	X	X
8.3.2	OSP-6		X	X	X	X
8.3.3	OSP-4 / OSP-3		X	X	X	X
9.1.1	OSP-12		X	X	X	X
9.1.2	OSP-16	X	X	X	X	X
9.2.1	OSP-12		X	X	X	X
9.2.2	OSP-12		X	X	X	X
9.2.3	OSP-12		X	X	X	X
9.2.4	OSP-12		X	X	X	X

ISO 27001	ISM3	Nivel 1: inicial	Nivel 2: Crecimiento	Nivel 3: Desarrollo	Nivel 4: Madurez	Nivel 5: Optimizado
9.2.5	OSP-12		X	X	X	X
9.2.6	OSP-12		X	X	X	X
9.3.1	OSP-12		X	X	X	X
9.4.1	OSP-12		X	X	X	X
9.4.2	OSP-12		X	X	X	X
9.4.3	OSP-12		X	X	X	X
9.4.4	OSP-12		X	X	X	X
9.4.5	OSP-12		X	X	X	X
10.1.1	OSP-11		X	X	X	X
10.1.2	OSP-11		X	X	X	X
11.1.1	OSP-11		X	X	X	X
11.1.2	OSP-11		X	X	X	X
11.1.3	OSP-11		X	X	X	X
11.1.4	OSP-14		X	X	X	X
11.1.5	OSP-11		X	X	X	X
11.1.6	OSP-11		X	X	X	X
11.2.1	OSP-14		X	X	X	X
11.2.2	OSP-14		X	X	X	X
11.2.3	OSP-14		X	X	X	X
11.2.4	OSP-4		X	X	X	X
11.2.5	OSP-11		X	X	X	X
11.2.6	OSP-4 / OSP-3 / OSP-7 / TSP-13		X	X	X	X
11.2.7	OSP-4 / OSP-3 / OSP-6		X	X	X	X
11.2.8	TSP-11 / TSP-9		X	X	X	X
11.2.9	TSP-11 / TSP-9		X	X	X	X
12.1.1	GP-1	X	X	X	X	X
12.1.2	OSP-11 / OSP-12 / OSP-4		X	X	X	X
12.1.3	TSP-4			X	X	X
12.1.4	GP-3 /	X	X	X	X	X

ISO 27001	ISM3	Nivel 1: inicial	Nivel 2: Crecimiento	Nivel 3: Desarrollo	Nivel 4: Madurez	Nivel 5: Optimizado
	OSP-16					
12.2.1	OSP-17	X	X	X	X	X
12.3.1	OSP-10	X	X	X	X	X
12.4.1	OSP-11 /OSP-12 /OSP-17 /OSP-19 /OSP-23 /OSP-27 /OSP-28	X	X	X	X	X
12.4.2	OSP-11 / OSP-12 /OSP-27		X	X	X	X
12.4.3	OSP-11 / OSP-12 /OSP-23 /OSP-27		X	X	X	X
12.4.4	OSP-4		X	X	X	X
12.5.1	OSP-4		X	X	X	X
12.6.1	OSP-22 /OSP-5 / OSP-7	X	X	X	X	X
12.6.2	OSP-8			X	X	X
12.7.1	OSP-17 / OSP-19	X	X	X	X	X
13.1.1	OSP-16	X	X	X	X	X
13.1.2	TSP-4			X	X	X
13.1.3	OSP-16	X	X	X	X	X
13.2.1	GP-1 / TSP-3	X	X	X	X	X
13.2.2	GP-1 / TSP-4	X	X	X	X	X
13.2.3	OSP-11 / OSP-12	X	X	X	X	X
13.2.4	GP-1	X	X	X	X	X
14.1.1	OSP-8			X	X	X
14.1.2	OSP-11 / OSP-12 /	X	X	X	X	X

ISO 27001	ISM3	Nivel 1: inicial	Nivel 2: Crecimiento	Nivel 3: Desarrollo	Nivel 4: Madurez	Nivel 5: Optimizado
	OSP-16 / OSP-5 / OSP-7 / OSP-8					
14.1.3	OSP-11 / OSP-12 / OSP-16 / OSP-5 / OSP-7 / OSP-8	X	X	X	X	X
14.2.1	OSP-8			X	X	X
14.2.2	OSP-4		X	X	X	X
14.2.3	OSP-4		X	X	X	X
14.2.4	OSP-4		X	X	X	X
14.2.5	TSP-6		X	X	X	X
14.2.6	OSP-8			X	X	X
14.2.7	OSP-8 / TSP-4			X	X	X
14.2.8	OSP-4		X	X	X	X
14.2.9	OSP-4		X	X	X	X
14.3.1	OSP-11 / OSP-12		X	X	X	X
15.1.1	OSP-2		X	X	X	X
15.1.2	GP-1 (GP-018) / TSP-3	X	X	X	X	X
15.1.3	GP-2		X	X	X	X
15.2.1	TSP-4			X	X	X
15.2.2	TSP-4			X	X	X
16.1.1	All using the “Process Owner”	X	X	X	X	X
16.1.2	OSP-22		X	X	X	X
16.1.3	OSP-22		X	X	X	X
16.1.4	OSP-23 / OSP-28				X	X
16.1.5	OSP-24			X	X	X

ISO 27001	ISM3	Nivel 1: inicial	Nivel 2: Crecimiento	Nivel 3: Desarrollo	Nivel 4: Madurez	Nivel 5: Optimizado
16.1.6	OSP-24			X	X	X
16.1.7	OSP-25				X	X
17.1.1	OSP-15			X	X	X
17.1.2	OSP-15			X	X	X
17.1.3	OSP-15 / OSP-20			X	X	X
17.2.1	OSP-26				X	X
18.1.1	GP-3	X	X	X	X	X
18.1.2	GP-3	X	X	X	X	X
18.1.3	OSP-11 / OSP-12 / OSP-27		X	X	X	X
18.1.4	GP-3 / TSP-4	X	X	X	X	X
18.1.5	GP-3 / TSP-4	X	X	X	X	X
18.2.1	GP-2 / OSP-21		X	X	X	X
18.2.2	GP-2		X	X	X	X
18.2.3	OSP-17 / OSP-19	X	X	X	X	X

Cuadro 3.5 Controles de acuerdo al nivel de madurez.

3.3.7. Indicadores

Para cada nivel de interacción del servicio se deben establecer indicadores, lo cual permite a la entidad dar respuesta a las interrogantes de ¿cuán efectivo y eficiente son los controles de respuesta al riesgo y los establecidos en el modelo? y ¿qué niveles de implementación y madurez han sido alcanzados?.

Los indicadores tienen 02 características principales:

- Alineamiento: se refiere al grado de correlación o vinculación con la Intención.
- Viabilidad: Grado de factibilidad o de la capacidad para obtener valores confiables del Indicador (data) de manera periódica.

Dichos indicadores deben contar con las características siguientes:

- Nombre del indicador: descripción que permite identificarlo.
- Objetivo o propósito: intención de la medición que debe estar alineado con el objetivo del control.
- Métrica: método de medición objetiva o subjetiva establecido en una formula o ecuación con información viable.
- Responsable: encargado del control y aseguramiento de las metas establecidas.
- Oportunidad o periodo de medición: tiempo de medición o cálculo de una meta derivada o resultado final.
- Metas o rangos de control: son las medida base, medida derivada y resultado de medición.

A continuación se detallan los tipos de indicadores:

- Actividad: su propósito es identificar el número de resultados producidos en un periodo.
- Alcance: su propósito es determinar la proporción del entorno (procesos, actividades o activos) que esta protegido.
- Disponibilidad: su propósito es identificar la proporción del periodo que el proceso o actividad ha funcionado, la frecuencia y la duración de las interrupciones.
- Eficacia: su propósito es identificar la proporción de resultados producidos comparados con el máximo posible. Esto implica la comparación con un valor conocido (valor base)
- Calidad: su propósito es establecer un rango de seguridad aceptable para las entradas, actividades y salidas de los procesos.
- Eficiencia: su propósito es identificar la proporción de pérdidas evitadas comparadas con el costo del proceso.

Estos indicadores son obligatorios establecerlos desde el nivel 03 de madurez (ver Cuadro 3.6).

Tipo de indicador	Nivel		
	Desarrollo	Madurez	Optimizado
Actividad	X	X	X
Alcance	X	X	X
Disponibilidad	X	X	X
Eficacia	X	X	X
Calidad		X	X
Eficiencia			X

Cuadro 3.6 Tipo de indicador por nivel de madurez.

3.3.8. Métricas

Para cada indicador establecido en los niveles de interacción del servicio se deben establecer métricas que de acuerdo al cálculo propuesto se estime la situación o estado de la eficacia de los controles de seguridad.

Dichas métricas deben contar como mínimo con las características siguientes:

- Ecuación o formula de la métrica.
- Unidad de medida.
- Frecuencia de toma de la medida.
- Fuente u origen de datos.
- Cálculo de las metas propuestas vs actuales.

4 CAPITULO IV: ANÁLISIS DE DATOS Y CASO DE ESTUDIO "PROCESO DE ATENCIÓN DE DENUNCIAS"

En el presente capítulo se presentan los resultados y el correspondiente análisis de los datos obtenidos en la investigación realizada a entidades del sector público a través de encuesta y se describe la aplicación del *modelo propuesto* en el proceso denominado Atención de Denuncias de una Entidad de Control.

4.1. Presentación y análisis de datos

En este sección se presentan los resultados obtenidos en la investigación realizada a través de la encuesta (ver anexo A), respecto al nivel de valoración que las instituciones objeto de la investigación le atribuyen a la seguridad de la información para los procesos que brindan servicio de gobierno electrónico, primero: la organización y funciones para la gestión de la seguridad de la información, segundo: la importancia de establecer niveles de madurez de seguridad, tercero: la importancia de establecer controles, indicadores y métricas como parte del modelo desarrollado y por último sobre la importancia de implementación de los elementos del modelo.

4.1.1. Informaciones Básicas

a) Tasa de respuesta

La tasa de respuesta se define formalmente como el número de cuestionarios utilizada, dividido por la población total de encuestados,

según [Frohlich 2002]. Según este autor, uno de los factores principales para evaluar el éxito de una encuesta, es su tasa de respuesta, debido a tres factores:

1. Cuando es alto el porcentaje de encuestados que no responde, existe un alto riesgo de los resultados de la investigación tengan un sesgo alto;
2. Muchas pruebas estadísticas requieren un gran número de respuestas para ser adecuadamente utilizados; y
3. Una alta tasa de respuesta indica, indirectamente, la pertinencia y el rigor del estudio a los ojos de la comunidad académica y empresarial en forma general.

En tal sentido, debemos indicar que en este estudio, se enviaron 78 cuestionarios a diferentes entidades públicas (ver Cuadro 4.1) vía web (http://goo.gl/forms/aEKjeVtD5o) y se respondieron de manera eficaz y debidamente validados 69 de estos, lo que viene a representar una tasa de respuesta del 88.46%, considerada adecuada para este estudio.

N°	Entidad
1	Agencia de Promoción de la Inversión Privada (PROINVERSIÓN)
2	Agencia Peruana de Cooperación Internacional (APCI)
3	Autoridad Nacional del Servicio Civil (SERVIR)
4	Banco Central de Reserva del Perú (BCRP)
5	Centro Nacional de Planeamiento Estratégico (CEPLAN)
6	Comisión de Promoción del Perú para la Exportación y el Turismo (PROMPERU)
7	Comisión Nacional para el Desarrollo y Vida sin Drogas (DEVIDA)
8	Congreso de la República
9	Consejo Nacional de la Magistratura (CNM)
10	Corporación peruana de aeropuertos y aviación comercial s.a. (CORPAC)
11	Defensoría del Pueblo (DP)
12	Despacho Presidencial
13	Dirección Nacional de Inteligencia
14	Empresa Nacional de la Coca S.A (ENACO S.A)
15	Empresa Nacional de Puertos S.A. (ENAPU)
16	Fondo Mi vivienda (MIVIVIENDA)
17	Fondo Nacional de Desarrollo Pesquero (FONDEPES)
18	Fuero Militar Policial (Ex - Consejo Supremo de Justicia Militar) (FMP)
19	Instituto de Investigaciones de la Amazonia Peruana (IIAP)
20	Instituto del Mar del Perú (IMARPE)
21	Instituto Geográfico Nacional (IGN)

N°	Entidad
22	Instituto Geológico Minero y Metalúrgico (INGEMMET)
23	Instituto Nacional de Defensa Civil (INDECI)
24	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
25	Instituto Nacional de Enfermedades Neoplásicas (INEN)
26	Instituto Nacional de Estadística e Informática
27	Instituto Nacional de Oftalmología
28	Instituto Nacional de Radio y Televisión del Perú
29	Instituto Nacional de Salud
30	Instituto Nacional de Salud del Niño
31	Instituto Nacional de Salud Mental
32	Instituto Nacional Materno Perinatal
33	Instituto Peruano de Energía Nuclear
34	Instituto Tecnológico de la Producción
35	Jurado Nacional de Elecciones (JNE)
36	Ministerio de Agricultura y Riego
37	Ministerio de Comercio Exterior y Turismo
38	Ministerio de Cultura
39	Ministerio de Defensa
40	Ministerio de Desarrollo e Inclusión Social
41	Ministerio de Economía y Finanzas
42	Ministerio de Educación
43	Ministerio de Energía y Minas
44	Ministerio de Justicia y Derechos Humanos
45	Ministerio de la Mujer y Poblaciones Vulnerables
46	Ministerio de la Producción
47	Ministerio de Relaciones Exteriores
48	Ministerio de Salud
49	Ministerio de Trabajo y Promoción del Empleo
50	Ministerio de Transportes y Comunicaciones
51	Ministerio de Vivienda, Construcción y Saneamiento
52	Ministerio del Ambiente
53	Ministerio del Interior
54	Ministerio Público Fiscalía de la Nación (MPFN)
55	Oficina Central de Lucha contra la Falsificación de Numerario (OCN)
56	Oficina de Normalización Previsional (ONP)
57	Oficina Nacional de Procesos Electorales (ONPE)
58	Oficina Nacional de Gobierno Electrónico e Informática (ONGEI)
59	Organismo de Formalización de la Propiedad Informal (COFOPRI)
60	Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre (OSINFOR)
61	Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)
62	Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN)
63	Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (OSITRAN)
64	Organismo Supervisor de las Contrataciones del Estado (OSCE)

N°	Entidad
65	Poder Judicial (PJ)
66	Policía Nacional del Perú (PNP)
67	Presidencia del Consejo de Ministros (PCM)
68	Registro Nacional de Identificación y Estado Civil (RENIEC)
69	Seguro Social de Salud (ESSALUD)
70	Servicios Postales del Perú S.A. (SERPOST)
71	Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS)
72	Superintendencia del Mercado de Valores (SMV)
73	Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT)
74	Superintendencia Nacional de Educación (SUNEDU)
75	Superintendencia Nacional de los Registros Públicos (SUNARP)
76	Superintendencia Nacional de Salud (SUNASA)
77	Superintendencia Nacional de Servicios de Saneamiento (SUNASS)
78	Tribunal Constitucional (TC)

Cuadro 4.1 Relación de las Instituciones encuestadas.

b) Datos faltantes

Asimismo, [Frohlich 2002] señala que la administración de los datos que faltan es una cuestión clave en una encuesta y no puede ser despreciada. Dicho autor propone que, para reducir al mínimo la presencia de datos faltantes, debe estar bien el diseño del cuestionario y debe proporcionar información clara a los encuestados, con el objetivo de aumentar su participación, pero advierte que aun así, inevitablemente, algunos datos faltarán.

El número total de cuestionarios que respondieron sin problemas fue de 69, ninguno de ellos presento datos que faltaban (no se permitía el envío si faltaba responder), por lo tanto ningún cuestionario resultó ser problemático y tampoco fue eliminado.

c) Datos extremos

Se entiende por datos extremos a aquellos que se desvían significativamente de las otras y puede influir indebidamente en el resultado de cualquier revisión y, de acuerdo con esto, el grado de influencia merece ser analizada.

En este trabajo de investigación se ha hecho una selección de organizaciones que de acuerdo a los criterios de la ONGEI deben implementar seguridad de la información, y por lo tanto podrían influir en el resultado de nuestra investigación.

Asimismo, para la valoración se ha considerado aplicar la escala de Likert, debido a que nos permite medir actitudes y conocer el grado de conformidad del encuestado con cualquier afirmación que le propongamos, evitando de esta manera las desviaciones.

En el presente trabajo de investigación no se obtuvo datos extremos, ya que todos se mantenían dentro del rango.

1. Definir la estructura organizacional y las funciones de los responsables de la seguridad de la información.
2. Identificar y establecer los niveles de madurez de seguridad de la información de acuerdo al tratamiento en el desarrollo de las fases del gobierno electrónico.
3. Establecer controles a implementar de acuerdo al nivel de madurez requerido en los procesos que brindan servicio de gobierno electrónico.
4. Establecer métricas e indicadores que permitan medir el desempeño de la gestión de seguridad en los servicios del gobierno electrónico.

4.1.2. Análisis de los Datos

En esta sección se muestra la estadística descriptiva de los datos recogidos.

Se realizó la recolección de información de 69 entidades del sector público (entidades comprendidas en la Resolución Ministerial 129 – 2012 –PCM y organismos autónomos) mediante una encuesta vía web (ver Anexo A) dirigida a encargados de seguridad de la información o Jefes

de Tecnologías de la información, en la que se validaron los objetivos, planteados (ver Cuadro 4.2).

Objetivo	Detalle del resultado de las preguntas	valor
General: Elaborar un modelo de gestión de seguridad de la información para el gobierno electrónico en las entidades públicas.	1. Se considera que se debe implementar la seguridad de la información en los procesos fundamentales. 2. Se debe considerar altamente la seguridad de la información como parte de la gestión de los procesos que brindan servicio de gobierno electrónico.	46 (66.7 %) Muy alta 52 (75.4%) Alta 17 (24.6%)
Específico a: Definir la estructura organizacional y las funciones de los responsables de la seguridad de la información.	3. Se debe organizar la gestión de seguridad de la información en todos los niveles (Estratégico, tácticos y operativo) 4. Se considera que las funciones de los responsables de la gestión de seguridad de la información deben ser establecidas en todos los niveles (Estratégico, tácticos y operativo)	69 (100 %) 68 (98.6 %)
Específico b: Identificar y establecer niveles de madurez de seguridad de la información.	5. Se cree altamente relevante contar con niveles de madurez establecidos que permitan identificar el estado de seguridad.	Muy alta 20 (29 %) Alta 49 (71%)
Específico c: Establecer controles a implementar de acuerdo al nivel de madurez requerido en los procesos que brindan servicio de gobierno electrónico.	6. Se cree altamente relevante contar documentos mínimos requeridos de acuerdo a los niveles de madurez establecidos. 7. Se cree altamente relevante contar controles de acuerdo a los niveles de madurez establecidos.	Muy alta 28 (41.8 %) Alta 39 (58.2 %) Muy alta 32 (46.4 %) Alta 37 (53.6 %)
Específico d: Establecer métricas e indicadores que permitan medir el desempeño de la gestión de seguridad en los servicios del gobierno electrónico.	8. Se cree altamente relevante contar indicadores que permitan monitorear los controles implementados. 9. Se cree altamente relevante contar métricas que permitan conocer la viabilidad de los controles implementados.	Muy alta 32 (46.4 %) Alta 37 (53.6 %) Muy alta 32 (46.4 %) Alta 37 (53.6 %)

Cuadro 4.2 Resumen de resultados de acuerdo a objetivos.

De la recolección de información de las entidades objeto de la investigación se evaluó la prioridad de contar con los elementos identificados en la revisión de los modelos (ver Cuadro 4.3).

N.°	Elementos	Muy prioritario
1	Estructura organizacional	65.0 (94.2%)
2	Funciones de los responsables.	64 (92.8%)
3	Fases para la implementación y operatividad.	62 (89.9%)
4	Niveles de madurez.	60 (87%)
5	Documentación.	64 (92.8%)
6	Controles.	65.0 (94.2%)
7	Indicadores.	61 (88.4%)
8	Métricas.	61 (88.4%)

Cuadro 4.3Prioridad de elementos identificados.

A continuación se detalla el análisis de cada una de las peguntas de la encuesta:

a) La organización y funciones para la gestión de la Seguridad de la información.

Con respecto al objetivo (a) definir la estructura organizacional y las funciones de los responsables de la seguridad de la información.

En general la seguridad de la información debe ser implementada en las entidades objeto del estudio: 13 (18.8 %) de ellas consideran que se debe implementar en los procesos estratégicos, 46 (66.7 %) consideran que se debe implementar en los procesos fundamentales y las otras 10 (14.5 %) consideran que se debe implementar en los procesos de apoyo (ver Figura 4.1).

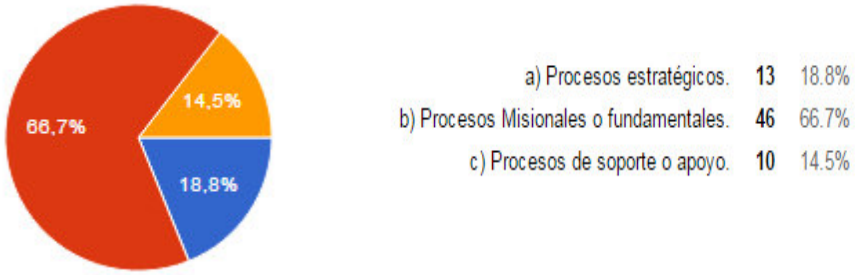


Figura 4.1 Procesos en donde se implementaría seguridad de la información.

Asimismo, respecto a la medida en que se debe considerar la seguridad de la información como parte de la gestión de los procesos que brindan servicio de gobierno electrónico: 52 (75.4%) de ellas consideran que debe ser muy alta y las otras 17 (24.6%) consideran que debe ser alta (ver Figura 4.2).

Figura 4.2 Implementar seguridad de la información en los procesos que brindan servicio de gobierno electrónico.

Luego de identificada la importancia de la seguridad de la información en las entidades objeto del estudio, se evalúa a qué nivel se debe organizar la gestión de seguridad de la información: 69 (100 %) consideran que debe ser en todos los niveles y ninguna considera que debe ser solo a nivel estratégico, nivel táctico o nivel operativo (ver Figura 4.3).

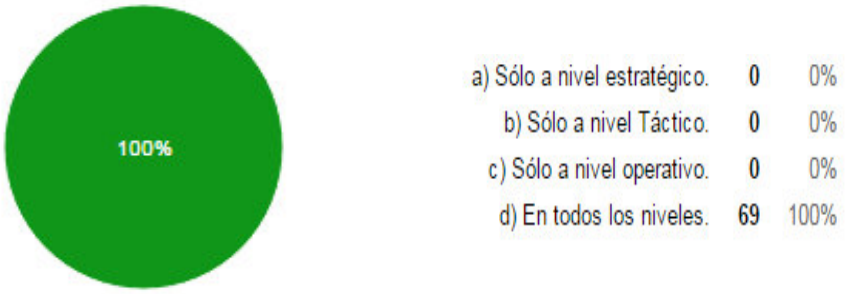


Figura 4.3 Organización de la gestión de seguridad de la información.

Y en cuanto a las funciones de los responsables de la gestión de seguridad de la información las entidades objeto del estudio consideran que deben ser establecidas: 68 (98.6 %) consideran que debe ser en todos los niveles, 1 (0.00 %) considera que debe ser a nivel táctico y ninguna considera que debe ser a solo a nivel estratégico o nivel operativo (ver Figura 4.4).

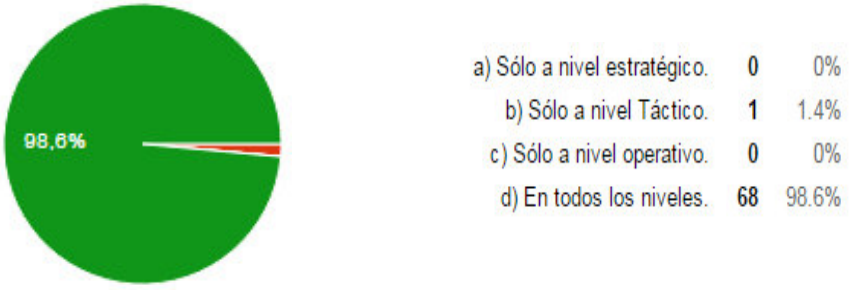


Figura 4.4 Funciones de los responsable de seguridad de la información.

b) La importancia de establecer niveles de madurez de seguridad.

En lo correspondiente al objetivo (b) identificar y establecer los niveles de madurez de seguridad de la información de acuerdo al tratamiento en el desarrollo de las fases del gobierno electrónico.

Las entidades objeto del estudio creen relevante contar con niveles de madurez establecidos que permitan identificar el estado de la seguridad: 20 (29 %) lo consideran muy alto, 49 (71%) lo consideran alto y ninguna lo consideran medio, bajo o muy bajo (ver Figura 4.5).

Figura 4.5 Contra con niveles de madurez de seguridad de la información.

c) La importancia de establecer controles, indicadores y métricas como parte del modelo desarrollado.

En lo correspondiente los objetivos (c) establecer controles a implementar de acuerdo al nivel de madurez requerido en los procesos que brindan servicio de gobierno electrónico y (d) establecer métricas e indicadores que permitan medir el desempeño de la gestión de seguridad en los servicios del gobierno electrónico.

Las entidades objeto del estudio creen relevante contar documentos y controles, de acuerdo a los niveles de madurez establecidos:

- Contar con documentos de acuerdo a los niveles de madurez 28 (41.8 %) lo considera muy alto, 39 (58.2 %) lo considera alto y ninguna lo consideran medio, bajo o muy bajo (ver Figura 4.6).

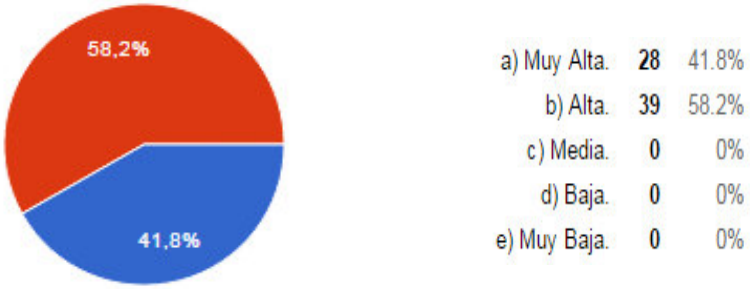


Figura 4.6 Contra con documentos de acuerdo a niveles de madurez.

- Contar con controles de acuerdo a los niveles de madurez

  32 (46.4 %) lo considera muy alto, 37 (53.6 %) lo considera alto y ninguna lo consideran medio, bajo o muy bajo (ver Figura 4.7).

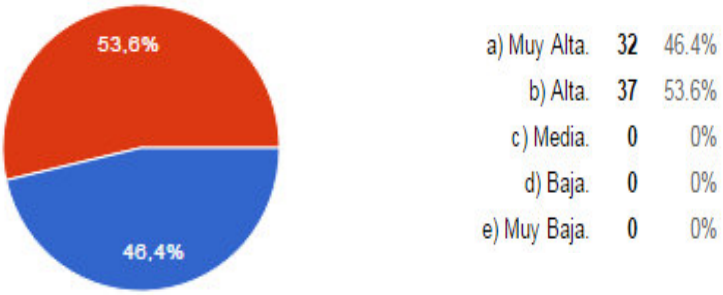


Figura 4.7 Contra con controles de acuerdo a niveles de madurez.

Y en cuanto a si creen relevante contar indicadores y métricas que permitan monitorear y conocer la viabilidad de los controles implementados.

- Contar con indicadores

  34 (49.3 %) lo considera muy alto, 35 (50.7%) lo considera alto y ninguna lo consideran medio, bajo o muy bajo (ver Figura 4.8).

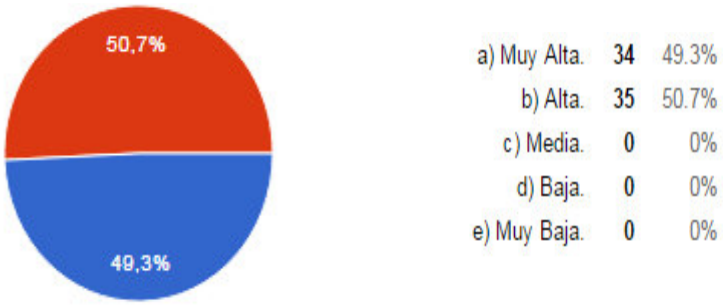


Figura 4.8 Contra con indicadores de acuerdo a los controles.

- Contar con métricas

  32 (46.4 %) lo considera muy alto, 36 (52.2 %) lo considera alto, 1 (1.4 %) lo consideran medio y ninguna lo considera bajo o muy bajo (ver Figura 4.9).

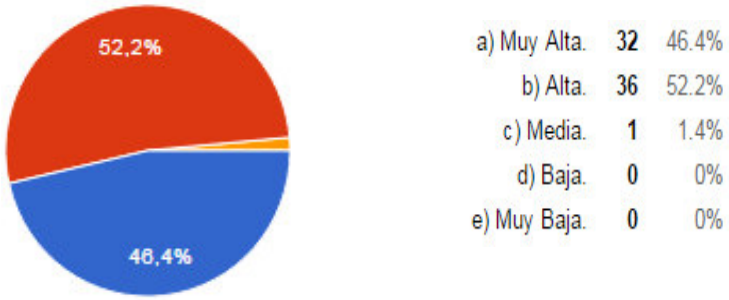


Figura 4.9 Contra con métricas de acuerdo a los indicadores.

d) La importancia de implementación de los elementos del modelo SGSI-EGob.

Las entidades objeto del estudio consideran muy prioritario los 08 elementos propuestos en el modelo (ver Cuadro 4.4).

		Prioritario		
N.°	**Elementos**	**1 (Muy prioritario)**	**2 (Medio prioritario)**	**3 (No es prioritario)**
1	Estructura organizacional	65.0 (94.2%)	4.0 (5.8%)	0 (0.0%)
2	Funciones de los responsables.	64 (92.8%)	5 (7.2%)	0 (0.0%)
3	Fases para la implementación y operatividad.	62 (89.9%)	6 (8.7%)	1 (1.4%)
4	Niveles de madurez.	60 (87%)	6 (8.7%)	3 (4.3%)
5	Documentación.	64 (92.8%)	5 (7.2%)	0.0 (0.0%)
6	Controles.	65.0 (94.2%)	4.0 (5.8%)	0 (0.0%)
7	Indicadores.	61 (88.4%)	7 (10.1%)	1 (1.4%)
8	Métricas.	61 (88.4%)	7 (10.1%)	1 (1.4%)

Cuadro 4.4 Importancia de los elemntos del modelo SGSI-E.Gob.

4.2. Caso de Estudio

4.2.1. Contexto de la Entidad de Control

a) Organización

La Entidad de Control creada en el año 1929 contaba inicialmente con un reducido equipo de colaboradores y tenía las funciones básicas de fiscalización preventiva del gasto público, llevar la contabilidad de la Nación, preparar la Cuenta General de la República e inspección a todas y cada una de las entidades públicas.

35 años más tarde, se le otorga a la entidad de control la calidad de Organismo autónomo con independencia administrativa y funcional, teniendo como función principal la de efectuar la supervisión, vigilancia y verificación de la correcta gestión y utilización de los recursos y bienes del Estado.

Es precisamente que a fin de llegar a más entidades públicas se ha implementado sedes en 24 provincias a nivel nacional, asimismo se dio inicio a una gestión bajo el enfoque por procesos.

b) Situación actual de la gestión de seguridad en el E-Gobierno.

La entidad de control, en la gestión bajo el enfoque por procesos ha establecido como uno de sus procesos fundamentales la atención de denuncias con la finalidad de captar mejor la demanda de la ciudadanía.

La atención de denuncias permite recibir y atender con celeridad las denuncias ciudadanas sobre presuntos actos de corrupción en la administración pública.

La atención de denuncias se encuentra organizada en 03 subprocesos (ver anexo B) y procedimientos, establecidos para desarrollar el tratamiento de las denuncias presentadas a nivel nacional, brindando los servicios de

gobierno electrónico en fase de interacción, a través de aplicaciones cliente servidor y web.

En los últimos años el crecimiento de la demanda de denuncias ha crecido de 1228 denuncias en el 2008 a 3745 en el 2014, es decir a un 20% anualmente aproximadamente.

De acuerdo a la demanda, se tiene el caso que el proceso de atención de denuncias recibe, procesa y emite cantidad de información física y digital, existiendo riesgos que puedan afectar dicha información y que los controles implementados no cumplan con la requerido o no sean eficaces, lo cual hace importante gestionar la seguridad de la información, principalmente en lo referido a la identidad del denunciante, el detalle y sustento de la denuncia, la suplantación de identidad de denunciante y la falsificación de documentación durante el proceso de atención de denuncias.

c) Problemática de la organización.

Según refiere el capítulo I donde se identifica la problemática del estudio de la presente tesis referida a que las entidades del sector público integrantes del Sistema Nacional de Informática no cuentan con un modelo de gestión de seguridad de la información que orienten la implementación y control de seguridad de la información.

4.2.2. Aplicación del MGSI-E-Gob.

a) Fases

1. Planear

La entidad de control ha realizado lo siguiente:

- Aprobó la política general de seguridad de la información.
- Aprobó los objetivos de seguridad del sistema de gestión de seguridad de la información.

- De acuerdo a los servicios de e-gobierno se estableció como alcance del sistema de gestión de seguridad de la información el proceso de Atención de denuncias.
- Estableció un procedimiento de gestión de Riesgos bajo el enfoque ISO 27005 e ISO 31000.
- La correspondiente al análisis y evaluación de riesgos, el plan de actividades y la asignación de recursos se detallan en el punto 4.4.6.

2. Hacer

La entidad de control ha realizado lo siguiente:

- Sensibilizó al personal de los procesos involucrados en el alcance y soporte del sistema de gestión de seguridad de la información sobre las medidas de seguridad implementadas
- Desarrolló un plan de actividades de los controles a implementar.
- Elaboró la documentación del SGSI.
- Definió los indicadores y métricas de los controles a implementar.
- Se dispuso a la Gerencia de Administración, Departamento de logística y Departamento de Personal brindar los recursos necesarios para la ejecución del plan de actividades.

3. Revisar

En esta fase la entidad ha realizado la revisión de la implementación y efectividad de los controles propuestos en el plan.

Sin embargo de requerir llegar a un nivel de madurez óptimo la entidad de control debe:

- Revisar el cumplimento de los Objetivos de seguridad de la información.
- Revisar la eficacia de los controles implementados

- Identificar las causas de las brechas de seguridad de la información
- Elaborar un plan de medidas correctivas.
- Mantener o ampliar el alcance del MGSI-EGob.

4. Actuar

Si la entidad de control requerir llegar a un nivel de madurez óptimo debe:

- Implementar las medidas correctivas.
- Ajustar los indicadores y métricas de los controles modificados o cambiados.

b) Organización

La entidad de control como parte del sistema de gestión integral (Calidad y Seguridad de la Información), ha definido una organización para la gestión de dicho sistema, la cual consta de un comité de gestión (alta dirección), un área operativa para cada sistema de gestión y responsables en cada uno de los procesos comprendidos en el alcance del SGSI (ver Figura 4.10).

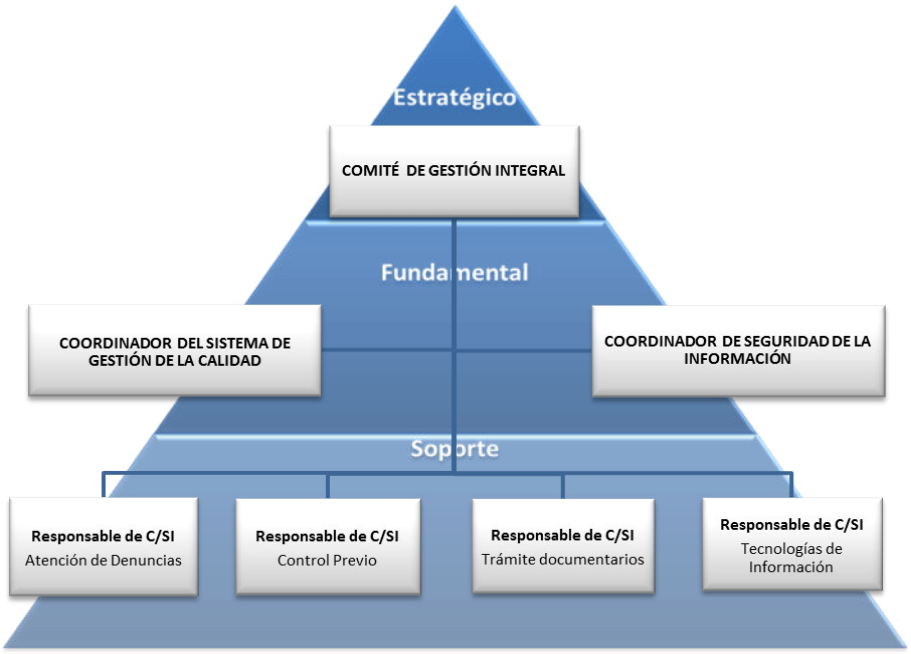


Figura 4.10 Estructura del sistema de gestión.

c) Funciones

Se ha definido funciones para cada uno de los responsables del sistema de gestión integral (Calidad y Seguridad de la Información), tal como se detallan en el Cuadro 4.5.

Estructura	Funciones
Estratégica	**Responsabilidades del Comité de Gestión Integral (CGI –C/SI)** a) Asegurar que las Políticas de la Calidad y de Seguridad de la Información sean entendida, implementada y mantenida en las unidades orgánicas de la CGR. b) Asegurar que se establecen los Objetivos de la Calidad y de Seguridad de la Información en las unidades orgánicas de la CGR. c) Evaluar la eficacia del Sistema de Gestión de la Calidad y Seguridad de la Información (SGC-SI) a través de las revisiones por la dirección. d) Asegurar la disponibilidad de los recursos necesarios para el SGC-SI. e) Informar al Contralor General los acuerdos tomados por el CGC-SI. f) Las demás que sean identificadas por el CGC-SI para la implementación, mantenimiento y mejora del SGC-SI.
	Responsabilidades del Presidente del CGC-C/SI a) Convocar y presidir las reuniones o sesiones de trabajo del CGC-SI y suscribir las actas de cada sesión conforme lo establecido en el SGC-SI; en caso de ausencia temporal, esta responsabilidad podrá ser delegada al Coordinador del Gestión de la Calidad y el Coordinador de Seguridad de la Información que corresponda según el tema a tratar. b) Asegurar que se establezcan, implementen y mantengan los procesos necesarios para el SGC-SI. c) Supervisar el adecuado y oportuno establecimiento, implementación y mantenimiento de la documentación general del SGC-SI. d) Informar al Contralor General sobre los problemas, obstáculos o inconvenientes que se presentan en el desarrollo e implementación del SGC-SI y promover con su apoyo las acciones de mejora que sean necesarias. e) Informar al Contralor General sobre el desempeño del SGC-SI y de cualquier necesidad de mejora, recomendándole las acciones que correspondan para su adecuado tratamiento. f) Asegurar que se promueva la sensibilización y toma de conciencia del cumplimiento de los requisitos del SGS-SI de los clientes en todos los niveles de la organización. g) Tomar las decisiones que correspondan al desarrollo, implementación y mejora continua del SGC-SI, en concordancia con las atribuciones que en el mismo sentido le hayan sido señaladas a otras instancias de la Contraloría General de la República. h) Otras que le sean asignadas por el Contralor General.
	Responsabilidades de los miembros del CGC-C/SI a) Asistir a las reuniones del CGC-SI con derecho a voz y voto.

Estructura	Funciones
	b) Proponer al CGC-SI los temas que consideren necesarios para su tratamiento y/o revisión. c) Analizar con anticipación los asuntos y documentos que serán tratados en las reuniones. d) Participar activamente en el análisis y discusión de los asuntos a tratar en las reuniones, así como realizar las tareas que el CGC-SI les encomiende. e) Informar del desarrollo y avance de las comisiones que les hayan sido conferidas. f) Asegurar el cumplimiento de los acuerdos tomados en el ámbito de su competencia. g) Representar a su unidad orgánica y sus dependencias en el CGC-SI. h) Comunicar a su unidad orgánica y sus dependencias lo tratado en el CGC-SI. i) Las demás que determine el CGC-SI.
Fundamental	**Responsabilidades del Coordinador del Sistema de Gestión de la Calidad y Coordinador de Seguridad de la Información** Los Coordinadores tendrán en sus respectivos campos de aplicación las siguientes responsabilidades: a) Presidir las reuniones o sesiones de trabajo del CGC-SI en caso de ausencia temporal del Presidente del Comité. b) Supervisar la difusión de la Política y Objetivos de la Calidad del CGC-SI. c) Coordinar la implementación, mejora y mantenimiento del CGC-SI. d) Convocar a reuniones, por encargo del Presidente del Comité o en ausencia de este; y preparar las actas de cada reunión. e) Organizar y custodiar la documentación que genere el CGC-SI. f) Programar las agendas y reuniones para la revisión del SGC por parte del CGC-SI. g) Apoyar y asesorar al CGC-SI. h) Las demás que sean identificadas por el Presidente del Comité.
Operativo	**Responsables de C/SI** Personal designado a nivel de unidad orgánica, área o proceso. Las funciones de los coordinadores de Seguridad de la Información son las siguientes: a) Implementar controles. b) Proponer al comité operativo los temas de seguridad de la información que considere necesarios para su tratamiento y/o revisión. c) Informar del desarrollo y avance de los equipos que les hayan sido conferidos. d) Representar a su unidad orgánica y sus dependencias ante el Comité Operativo. e) Comunicar a su unidad orgánica y dependencias la situación de la seguridad de la información bajo su ámbito. f) Evaluar la eficacia de los controles bajo su ámbito. g) Informar sobre los incidentes de seguridad al comité operativo. h) Tomar acciones inmediatas. i) Reportar periódicamente al Comité Operativo la situación de la seguridad de la información.

Cuadro 4.5 Funciones de los responsables del sistema de gestión integral C/SI.

d) Documentos

Como parte de los requisitos del sistema de gestión de seguridad de la información y del resultado de la evaluación de riesgos la entidad de control ha elaborado y aprobado los documentos propuestos como obligatorios por el modelo (ver Cuadro 4.6).

Documento	Detalle	Versión del documento
1. Alcance del SGSI	Comprende 03 subprocesos del proceso de atención de denuncias	Manual del sistema de gestión. (MC-SGI-01)
2. Políticas y objetivos de seguridad de la información	Política general y objetivos del sistema de Gestión de Seguridad de la Información.	MC-SGI-01: Manual del sistema de gestión. Resolución de Política General de SI.
3. Metodología de evaluación y tratamiento de riesgos	Se detalla cómo realizar el inventario de activos de información, la identificación de riesgos del entorno interno y externo, el análisis y la evaluación de riesgos y el plan de tratamiento de riesgos.	PRSEG 04: Procedimientos de gestión de riesgos en seguridad de la información.
4. Declaración de aplicabilidad	Detalla la justificación de la implementación y no implementación de controles.	F07 (PR-GSEG-04): Formato de aceptación del riesgo.
5. Plan de tratamiento del riesgo	Plan de implementación de controles de seguridad, responsables y periodo de implementación.	F06 (PR-GSEG-04): Formato de plan de tratamiento.
6. Informe sobre evaluación y tratamiento de riesgos	Matriz de riesgos inherentes y residuales	F04 (PR-GSEG-04): Formato de análisis de riesgos. F05 (PR-GSEG-04): Formato de evaluación de riesgos.
7. Procedimiento para control de documentos	Se detalla el control de documentos del sistema de gestión de riesgo.	PRG-SGI-01: Procedimientos de control de documentos. (de acuerdo a la directiva organización y emisión de documentos normativos v2)
8. Controles para gestión de registros	Se detalla el control de los registros de seguridad de la información.	F01 (PR-SGC-01): Lista maestra de documentos internos. F01 (PR-SGC-03): Matriz de control de registros. (ambos de acuerdo al

Documento	Detalle	Versión del documento
		PRG-SGI-01)
9. Procedimiento para auditoría interna	Se detalla el programa y ejecución de auditorías internas.	PRG-SGI-04: Procedimientos de auditorías internas.
10. Procedimiento para medidas correctivas	Se detalla la evaluación de la problemática, las medidas a implementar, los responsables y periodo de implementación.	PRG-SGI-05: Procedimientos de acciones correctivas y preventivas.

Cuadro 4.6 Documentos del sistema de gestión integral C/SI.

e) Niveles

El proceso de atención de denuncias presta el servicio de e-gobierno con tipo de relación Gobierno a Ciudadano en la fase de interacción, para lo cual la entidad de control determinó aplicar el modelo GSI-EGob en el nivel de madurez 3 (desarrollo).

f) Controles

Para poder determinar los controles a implementar la entidad de control ha aplicado la metodología de gestión de riesgos (ver anexos C, D, E, F y G) al proceso de atención de denuncias, tal como se muestra en el Cuadro 4.7.

Elementos de la metodología	Detalle
Sub proceso	03 sub procesos (Admisión, validación y atención de casos)
Inventario de activos	Se han identificado 38 activos de información.
Valorización de activos	Se han identificado: 25 de nivel bajo (valores de 1.00 a 2.99). 09 de nivel medio (valores de 3.00 a 3.99) 04 de nivel alto (valores de 4.00 a 5.0),
Riesgos	Se han identificado 08 riesgos.
Amenazas	Se han identificado: 04 amenazas con probabilidad de ocurrencia muy baja (valor 1) 04 amenazas con probabilidad de ocurrencia baja (valor 2) 05 amenazas con probabilidad de ocurrencia alto (valor 4) 02 amenazas con probabilidad de ocurrencia alto (valor 5)

Vulnerabilidades	Se han identificado: 01 vulnerabilidad con nivel muy bajo (valor 1) 02 vulnerabilidades con nivel bajo (valor 2) 12 vulnerabilidades con nivel medio (valor 3) 09 vulnerabilidades con nivel alto (valor 4)
Análisis de riesgos	Se han identificado: 01 riesgo de con probabilidad de ocurrencia de nivel muy bajo (o aceptable). 01 riesgo de con probabilidad de ocurrencia de nivel bajo. 04 riesgos de con probabilidad de ocurrencia de nivel medio. 03 riesgos de con probabilidad de ocurrencia de nivel alto.
Evaluación de riesgos.	Se han identificado: (ver Figura 4.11) 01 riesgo inherente de nivel bajo. 05 riesgos inherentes de nivel medio. 02 riesgos inherentes de nivel alto.
Opciones de tratamiento de riesgos	Se han propuesto controles a fin de mitigar el riesgo.
Análisis y evaluación de riesgos posterior a la implementación de controles.	Se han identificado: (ver Figura 4.12) 08 riesgos residuales de nivel muy bajo (o aceptable).

Cuadro 4.7 Resumen de resultados de evaluación de riesgos.

Criterios		Probabilidad de explotación				
		1 - 5	6 - 10	11 - 15	16 - 20	21 - 25
Impacto	1	Muy Bajo	Muy Bajo	Bajo	Bajo	Medio
	2	Muy Bajo **R1**	Bajo	Medio **R8**	Medio **R4** **R6**	Alto
	3	Bajo	Medio **R5**	Medio **R7**	Alto **R2** **R3**	Alto
	4	Bajo	Medio	Alto	Alto	Muy Alto
	5	Medio	Alto	Alto	Muy Alto	Muy Alto

Figura 4.11 Mapa de calor de riesgos inherentes.

Criterios		Probabilidad de explotación				
		1 - 5	6 - 10	11 - 15	16 - 20	21 - 25
Impacto	1	Muy Bajo **R2** **R8**	Muy Bajo **R7** **R3** **R5**	Bajo	Bajo	Medio
	2	Muy Bajo **R1** **R4** **R6**	Bajo	Medio	Medio	Alto
	3	Bajo	Medio	Medio	Alto	Alto
	4	Bajo	Medio	Alto	Alto	Muy Alto
	5	Medio	Alto	Alto	Muy Alto	Muy Alto

Figura 4.12 Mapa de calor de riesgos residuales.

Luego de la aplicación de la metodología de gestión de riesgo, se ha elaborado el documento de declaración de aplicabilidad, en el cual se ha justificado los controles que se va a implementar y los que no (ver Cuadro 4.8).

Dominio	Controles	
	Implementar	No Implementar
A.5 Políticas de seguridad de la información	2	0
A.6 Organización de la seguridad de la información	5	2
A.7 Seguridad de los recursos humanos	6	0
A.8 Gestión de activos	10	0
A.9 Control de acceso	14	0
A.10 Criptografía	2	0
A.11 Seguridad física y ambiental	15	0
A.12 Seguridad de las operaciones	14	0
A.13 Seguridad de las comunicaciones	7	0
A.14 Adquisición, desarrollo y mantenimiento del sistema	13	0
A.15 Relaciones con los proveedores	5	0
A.16 Gestión de incidentes de seguridad de la información	7	0
A.17 Aspectos de seguridad de la información en torno a la gestión de continuidad del negocio	4	0
A.18 Cumplimiento	8	0

Cuadro 4.8 Resumen de Controles a implementar por dominio.

Como parte de los requisitos de seguridad de la información y del resultado de la evaluación de riesgos del proceso de atención de denuncias, se ha actualizado e implementado los controles requeridos, de los cuales se ha realizado una evaluación de acuerdo a lo establecido por el modelo GSI-E-Gob en el nivel de madurez 3 o definido (ver Figura 4.13).

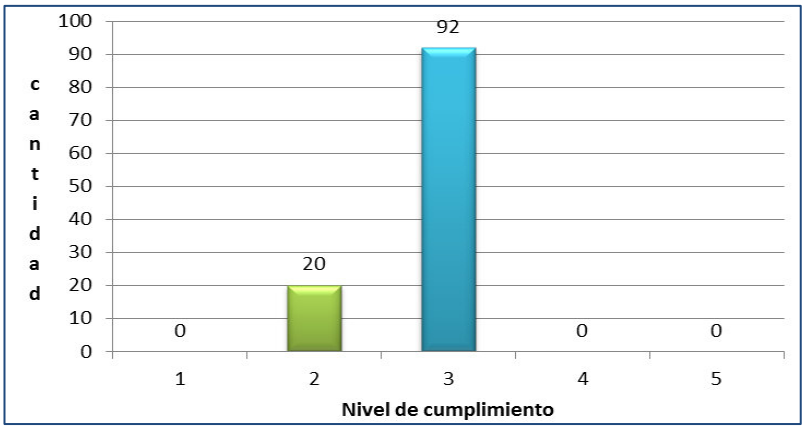


Figura 4.13 Nivel de cumplimiento de controles implementados.

Posteriormente se determinó el nivel de cumplimiento alcanzado por los controles del proceso de atención de denuncias (ver Cuadro 4.9).

Controles	Nivel
5.1.1 Conjunto de políticas para la seguridad de la información.	3
5.1.2 Revisión de las políticas para la seguridad de la información.	3
6.1.1 Asignación de responsabilidades para la segur. de la información.	3
6.1.2 Segregación de tareas.	3
6.1.3 Contacto con las autoridades.	3
6.1.4 Contacto con grupos de interés especial.	3
6.1.5 Seguridad de la información en la gestión de proyectos.	3
7.1.1 Investigación de antecedentes.	3
7.1.2 Términos y condiciones de contratación.	3
7.2.1 Responsabilidades de gestión.	3
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3
7.2.3 Proceso disciplinario.	3
7.3.1 Cese o cambio de puesto de trabajo.	3
8.1.1 Inventario de activos.	3
8.1.2 Propiedad de los activos.	3
8.1.3 Uso aceptable de los activos.	3

Controles	Nivel
8.1.4 Devolución de activos.	3
8.2.1 Directrices de clasificación.	3
8.2.2 Etiquetado y manipulado de la información.	2
8.2.3 Manipulación de activos.	2
8.3.1 Gestión de soportes extraíbles.	3
8.3.2 Eliminación de soportes.	2
8.3.3 Soportes físicos en tránsito.	2
9.1.1 Política de control de accesos.	3
9.1.2 Control de acceso a las redes y servicios asociados.	3
9.2.1 Gestión de altas/bajas en el registro de usuarios.	3
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	3
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	3
9.2.4 Gestión de información confidencial de autenticación de usuarios.	3
9.2.5 Revisión de los derechos de acceso de los usuarios.	3
9.2.6 Retirada o adaptación de los derechos de acceso	3
9.3.1 Uso de información confidencial para la autenticación.	3
9.4.1 Restricción del acceso a la información.	3
9.4.2 Procedimientos seguros de inicio de sesión.	3
9.4.3 Gestión de contraseñas de usuario.	2
9.4.4 Uso de herramientas de administración de sistemas.	3
9.4.5 Control de acceso al código fuente de los programas.	3
10.1.1 Política de uso de los controles criptográficos.	3
10.1.2 Gestión de claves.	2
11.1.1 Perímetro de seguridad física.	3
11.1.2 Controles físicos de entrada.	3
11.1.3 Seguridad de oficinas, despachos y recursos.	3
11.1.4 Protección contra las amenazas externas y ambientales.	3
11.1.5 El trabajo en áreas seguras.	3
11.1.6 Áreas de acceso público, carga y descarga.	3
11.2.1 Emplazamiento y protección de equipos.	3
11.2.2 Instalaciones de suministro.	3
11.2.3 Seguridad del cableado.	3
11.2.4 Mantenimiento de los equipos.	3
11.2.5 Salida de activos fuera de las dependencias de la empresa.	3
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	3
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	3
11.2.8 Equipo informático de usuario desatendido.	3
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	3
12.1.1 Documentación de procedimientos de operación.	3
12.1.2 Gestión de cambios.	2
12.1.3 Gestión de capacidades.	2
12.1.4 Separación de entornos de desarrollo, prueba y producción.	3
12.2.1 Controles contra el código malicioso.	3
12.3.1 Copias de seguridad de la información.	3
12.4.1 Registro y gestión de eventos de actividad.	3
12.4.2 Protección de los registros de información.	3
12.4.3 Registros de actividad del administrador y operador del sistema.	2
12.4.4 Sincronización de relojes.	3
12.5.1 Instalación del software en sistemas en producción.	2
12.6.1 Gestión de las vulnerabilidades técnicas.	3
12.6.2 Restricciones en la instalación de software.	2

Controles	Nivel
12.7.1 Controles de auditoría de los sistemas de información.	3
13.1.1 Controles de red.	3
13.1.2 Mecanismos de seguridad asociados a servicios en red.	3
13.1.3 Segregación de redes.	3
13.2.1 Políticas y procedimientos de intercambio de información.	3
13.2.2 Acuerdos de intercambio.	3
13.2.3 Mensajería electrónica.	3
13.2.4 Acuerdos de confidencialidad y secreto.	3
14.1.1 Análisis y especificación de los requisitos de seguridad.	2
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	2
14.1.3 Protección de las transacciones por redes telemáticas.	3
14.2.1 Política de desarrollo seguro de software.	3
14.2.2 Procedimientos de control de cambios en los sistemas.	3
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	3
14.2.4 Restricciones a los cambios en los paquetes de software.	3
14.2.5 Uso de principios de ingeniería en protección de sistemas.	3
14.2.6 Seguridad en entornos de desarrollo.	2
14.2.7 Externalización del desarrollo de software.	2
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.	2
14.2.9 Pruebas de aceptación.	3
14.3.1 Protección de los datos utilizados en pruebas.	3
15.1.1 Política de seguridad de la información para suministradores.	3
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	3
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	3
15.2.1 Supervisión y revisión de los servicios prestados por terceros.	3
15.2.2 Gestión de cambios en los servicios prestados por terceros.	3
16.1.1 Responsabilidades y procedimientos.	3
16.1.2 Notificación de los eventos de seguridad de la información.	3
16.1.3 Notificación de puntos débiles de la seguridad.	3
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	3
16.1.5 Respuesta a los incidentes de seguridad.	3
16.1.6 Aprendizaje de los incidentes de seguridad de la información.	3
16.1.7 Recopilación de evidencias.	3
17.1.1 Planificación de la continuidad de la seguridad de la información.	2
17.1.2 Implantación de la continuidad de la seguridad de la información.	2
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	3
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	2
18.1.1 Identificación de la legislación aplicable.	3
18.1.2 Derechos de propiedad intelectual (DPI).	3
18.1.3 Protección de los registros de la organización.	3
18.1.4 Protección de datos y privacidad de la información personal.	3
18.1.5 Regulación de los controles criptográficos.	2
18.2.1 Revisión independiente de la seguridad de la información.	3
18.2.2 Cumplimiento de las políticas y normas de seguridad.	3
18.2.3 Comprobación del cumplimiento.	3

Cuadro 4.9 Resumen de nivel de cumplimiento de controles.

g) Indicadores

Para los controles a implementarse en el nivel de madurez 3 (definido) del MGSI-E-Gob no se obliga el establecimiento de indicadores; sin embargo dependiendo de los controles implementados, la entidad ha establecido indicadores de tipo actividad, alcance, disponibilidad, eficacia y calidad (ver Cuadros 4.10 y 4.11), en 92 de 112 controles (ver Figura 4.14).

Controles	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
43 controles con 1 indicador	6	32	1	0	4
38 controles con 2 indicadores	26	29	3	13	5
8 controles con 3 indicadores	8	7	1	6	2
3 controles con 4 indicadores	3	3	3	3	0
Total indicadores	**43**	**71**	**8**	**22**	**11**

Cuadro 4.10 Tipo de indicadores por control.

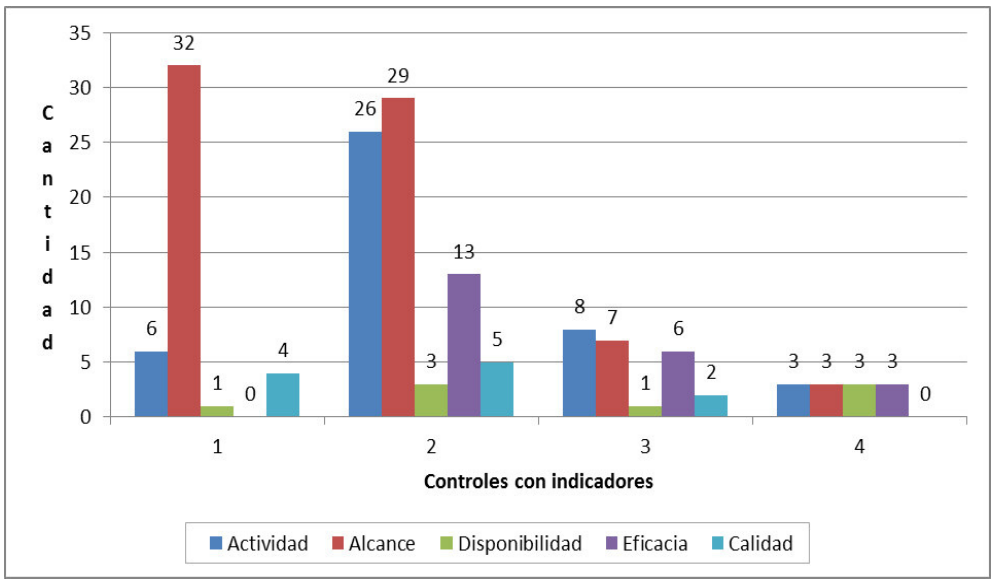


Figura 4.14 Controles con 1, 2, 3 o 4 indicadores.

Control	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
5.1.1 Conjunto de políticas para la seguridad de la información.		X			
5.1.2 Revisión de las políticas para la seguridad de la información.		X		X	
6.1.1 Asignación de responsabilidades para la segur. de la información.		X			
6.1.2 Segregación de tareas.		X			X
6.1.3 Contacto con las autoridades.		X			
6.1.4 Contacto con grupos de interés especial.		X			
6.1.5 Seguridad de la información en la gestión de proyectos.	X	X			
7.1.1 Investigación de antecedentes.					X
7.1.2 Términos y condiciones de contratación.	X			X	X
7.2.1 Responsabilidades de gestión.		X			
7.2.2 Concienciación, educación y capacitación en seguridad de la información.					X
7.2.3 Proceso disciplinario.					X
7.3.1 Cese o cambio de puesto de trabajo.		X			
8.1.1 Inventario de activos.	X	X			
8.1.2 Propiedad de los activos.	X				
8.1.3 Uso aceptable de los activos.		X	X		
8.1.4 Devolución de activos.		X	X		
8.2.1 Directrices de clasificación.		X			
8.2.2 Etiquetado y manipulado de la información.					
8.2.3 Manipulación de activos.					
8.3.1 Gestión de soportes extraíbles.		X			
8.3.2 Eliminación de soportes.					
8.3.3 Soportes físicos en tránsito.					
9.1.1 Política de control de accesos.		X			
9.1.2 Control de acceso a las redes y servicios asociados.	X	X		X	
9.2.1 Gestión de altas/bajas en el registro de usuarios.	X	X	X	X	
9.2.2 Gestión de los derechos de acceso asignados a usuarios.	X	X	X	X	

Control	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
9.2.3 Gestión de los derechos de acceso con privilegios especiales.	X	X	X	X	
9.2.4 Gestión de información confidencial de autenticación de usuarios.					X
9.2.5 Revisión de los derechos de acceso de los usuarios.	X	X		X	
9.2.6 Retirada o adaptación de los derechos de acceso	X	X		X	
9.3.1 Uso de información confidencial para la autenticación.	X	X			
9.4.1 Restricción del acceso a la información.	X	X			
9.4.2 Procedimientos seguros de inicio de sesión.		X			X
9.4.3 Gestión de contraseñas de usuario.					
9.4.4 Uso de herramientas de administración de sistemas.	X	X			X
9.4.5 Control de acceso al código fuente de los programas.	X			X	
10.1.1 Política de uso de los controles criptográficos.		X			
10.1.2 Gestión de claves.					
11.1.1 Perímetro de seguridad física.		X			
11.1.2 Controles físicos de entrada.		X			
11.1.3 Seguridad de oficinas, despachos y recursos.		X			
11.1.4 Protección contra las amenazas externas y ambientales.	X	X			
11.1.5 El trabajo en áreas seguras.		X			
11.1.6 Áreas de acceso público, carga y descarga.		X			
11.2.1 Emplazamiento y protección de equipos.	X	X			
11.2.2 Instalaciones de suministro.	X			X	
11.2.3 Seguridad del cableado.		X			
11.2.4 Mantenimiento de los equipos.	X			X	
11.2.5 Salida de activos fuera de las dependencias de la empresa.	X			X	
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.		X			

Control	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	X			X	
11.2.8 Equipo informático de usuario desatendido.	X		X		
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.		X			
12.1.1 Documentación de procedimientos de operación.		X			X
12.1.2 Gestión de cambios.					
12.1.3 Gestión de capacidades.					
12.1.4 Separación de entornos de desarrollo, prueba y producción.		X			
12.2.1 Controles contra el código malicioso.	X			X	
12.3.1 Copias de seguridad de la información.	X	X			
12.4.1 Registro y gestión de eventos de actividad.	X	X			
12.4.2 Protección de los registros de información.	X	X			
12.4.3 Registros de actividad del administrador y operador del sistema.					
12.4.4 Sincronización de relojes.	X	X			
12.5.1 Instalación del software en sistemas en producción.					
12.6.1 Gestión de las vulnerabilidades técnicas.	X			X	
12.6.2 Restricciones en la instalación de software.					
12.7.1 Controles de auditoría de los sistemas de información.		X			
13.1.1 Controles de red.		X			
13.1.2 Mecanismos de seguridad asociados a servicios en red.		X			
13.1.3 Segregación de redes.	X				
13.2.1 Políticas y procedimientos de intercambio de información.		X			X
13.2.2 Acuerdos de intercambio.		X			
13.2.3 Mensajería electrónica.	X	X		X	
13.2.4 Acuerdos de confidencialidad	X	X		X	

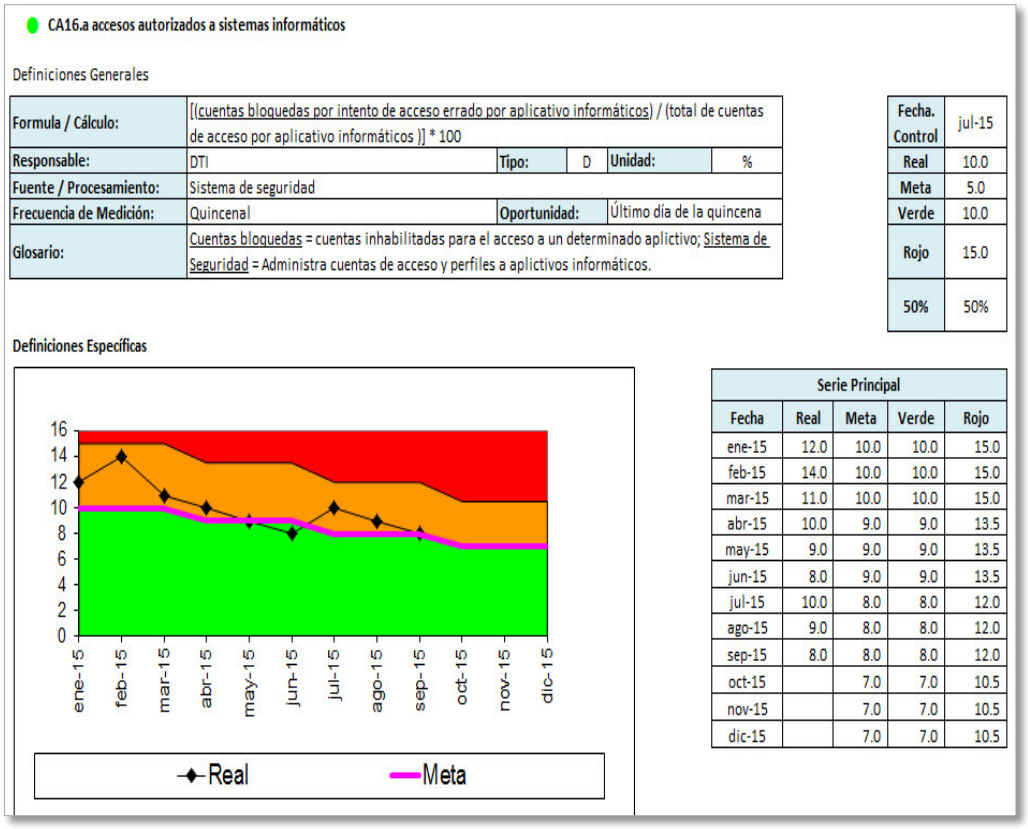
Control	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
y secreto.					
14.1.1 Análisis y especificación de los requisitos de seguridad.					
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.					
14.1.3 Protección de las transacciones por redes telemáticas.	X	X			
14.2.1 Política de desarrollo seguro de software.		X			
14.2.2 Procedimientos de control de cambios en los sistemas.		X			X
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.		X		X	
14.2.4 Restricciones a los cambios en los paquetes de software.	X	X			
14.2.5 Uso de principios de ingeniería en protección de sistemas.	X	X			
14.2.6 Seguridad en entornos de desarrollo.					
14.2.7 Externalización del desarrollo de software.					
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.					
14.2.9 Pruebas de aceptación.	X	X			
14.3.1 Protección de los datos utilizados en pruebas.	X	X			
15.1.1 Política de seguridad de la información para suministradores.		X			
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.		X			
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.		X			
15.2.1 Supervisión y revisión de los servicios prestados por terceros.		X		X	
15.2.2 Gestión de cambios en los servicios prestados por terceros.		X			
16.1.1 Responsabilidades y procedimientos.		X			
16.1.2 Notificación de los eventos de seguridad de la información.		X			
16.1.3 Notificación de puntos	X				

Control	Tipo de indicador				
	Actividad	Alcance	Disponibilidad	Eficacia	Calidad
débiles de la seguridad.					
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	X				
16.1.5 Respuesta a los incidentes de seguridad.	X	X	X		
16.1.6 Aprendizaje de los incidentes de seguridad de la información.		X			
16.1.7 Recopilación de evidencias.			X		
17.1.1 Planificación de la continuidad de la seguridad de la información.					
17.1.2 Implantación de la continuidad de la seguridad de la información.					
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		X		X	
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.					
18.1.1 Identificación de la legislación aplicable.	X				
18.1.2 Derechos de propiedad intelectual (DPI).	X				
18.1.3 Protección de los registros de la organización.	X	X			
18.1.4 Protección de datos y privacidad de la información personal.	X	X			
18.1.5 Regulación de los controles criptográficos.					
18.2.1 Revisión independiente de la seguridad de la información.		X		X	
18.2.2 Cumplimiento de las políticas y normas de seguridad.	X			X	
18.2.3 Comprobación del cumplimiento.		X			

Cuadro 4.11 Controles con indicadores identificados.

h) Métricas

Las fichas de indicadores elaboradas para los controles implementados contemplan elementos como la formula, unidad de medida, frecuencia, oportunidad y metas planificadas y reales (ver Figura 4.15).



CA16.a accesos autorizados a sistemas informáticos

Definiciones Generales

Formula / Cálculo:	[(cuentas bloquedas por intento de acceso errado por aplicativo informáticos) / (total de cuentas de acceso por aplicativo informáticos)] * 100				
Responsable:	DTI	Tipo:	D	Unidad:	%
Fuente / Procesamiento:	Sistema de seguridad				
Frecuencia de Medición:	Quincenal	Oportunidad:		Último día de la quincena	
Glosario:	Cuentas bloquedas = cuentas inhabilitadas para el acceso a un determinado aplictivo; Sistema de Seguridad = Administra cuentas de acceso y perfiles a aplictivos informáticos.				

Fecha. Control	jul-15
Real	10.0
Meta	5.0
Verde	10.0
Rojo	15.0
50%	50%

Definiciones Específicas

Serie Principal				
Fecha	Real	Meta	Verde	Rojo
ene-15	12.0	10.0	10.0	15.0
feb-15	14.0	10.0	10.0	15.0
mar-15	11.0	10.0	10.0	15.0
abr-15	10.0	9.0	9.0	13.5
may-15	9.0	9.0	9.0	13.5
jun-15	8.0	9.0	9.0	13.5
jul-15	10.0	8.0	8.0	12.0
ago-15	9.0	8.0	8.0	12.0
sep-15	8.0	8.0	8.0	12.0
oct-15		7.0	7.0	10.5
nov-15		7.0	7.0	10.5
dic-15		7.0	7.0	10.5

Figura 4.15 Características de métricas de la ficha de indicador.

4.2.3. Evaluación de resultados.

a) Resultados de modelo vs. implementado.

Luego de realizada la implementación del modelo GSI-EGob en la Entidad de Control durante el periodo Octubre 2014 a Octubre 2015, el cuadro 4.12, muestra una evaluación comparativa de la implementación realizada versus lo planteado por el modelo.

Elementos	Comparación		
	MGSI-EGob	Real	Cumple / Observación
1. Niveles	**Definido**	Se seleccionó el nivel 3: **Definido**	**Cumple**
2. Fases	Plan / Do	Plan / Do	**Cumple**
3. Organización	Alta dirección designa responsable de SI.	Se cuenta con una estructura organizacional a nivel estratégico, táctico y operativo.	**Cumple**
4. Funciones	Definida del responsable de SI.	Cada integrante de la estructura organizacional cuenta con funciones definidas.	**Cumple**
5. Documento	10	Se cuenta con directivas, políticas, procedimientos y formatos referidos a seguridad de la información	**Cumple**
6. Controles	107	Se han implementado 112 controles de acuerdo a lo establecido en la declaración de aplicabilidad y gestión de riesgos realizada.	**Observación:** 92 controles cumplen con lo requerido.
7. Indicadores	4	Se han definido 5 tipos de indicadores (Actividad, Alcance, Disponibilidad, Eficacia y calidad) para los diferentes controles, contando con un total de 155 fichas de indicadores.	**Cumple**
8. Métricas	Por tipo de indicador	Las 155 fichas de indicadores cuentan con las características requeridas para las métricas.	**Cumple**

Cuadro 4.12 Comparativa de los elementos propuestos por el modelo versus lo implementado.

b) Resultados de situación actual vs. implementado.

La implementación del modelo GSI-EGob en la Entidad de Control permite comparar la situación actual a fines de octubre de 2014 vs. La situación actual a octubre 2015, el cuadro 4.13, muestra una evaluación comparativa de la implementación realizada versus lo planteado por el modelo.

Elementos	Comparación		
	Octubre 2014	Octubre 15	Observación
1. Niveles	No se conocía el nivel de seguridad	Se seleccionó el nivel 3: **Definido**	Se desconocía la brecha de seguridad.
2. Fases	Se contaba con Política de seguridad	Plan / Do	No se contaba con Objetivo y Alcance. No se contaba con un plan de implementación.
3. Organización	Se tenía sólo comité de seguridad a nivel de la dirección.	Se cuenta con una estructura organizacional a nivel estratégico, táctico y operativo.	No se contaba con responsables de seguridad a nivel operativo y táctico. La estructura organizacional es de 03 niveles.
4. Funciones	Las funciones definidas estaban desactualizadas y referidas a normativa de seguridad de la información y seguridad y salud en el trabajo.	Cada integrante de la estructura organizacional cuenta con funciones definidas.	Se tenían funciones generales y combinadas con otra norma.
5. Documento	Se contaba con documento de Política general de SI y la directiva organización y emisión de documentos normativos (versión 1.0) como parte del control de documentos	Se cuenta con directivas, políticas, procedimientos y formatos referidos a seguridad de la información	Se desconocía y no se contaba con la documentación requerida mínima. Teniendo actualmente el 100% de la documentación vigente, actualizada y controlada.
6. Controles	Se tenían 65 controles, no pudiendo medir su nivel de cumplimiento por no contar con indicadores y métricas y muchos de ellos no contaban con registros.	Se han implementado 112 controles de acuerdo a lo establecido en la declaración de aplicabilidad y gestión de riesgos realizada.	Los controles con los que se contaban, no eran monitoreados por no contar con indicadores y metas. Se incrementó el 58% faltante de controles.
7. Indicadores	No se cuenta con indicadores	Se han definido 5 tipos de indicadores (Actividad, Alcance, Disponibilidad, Eficacia y calidad) para los diferentes controles, contando con un total de 155 fichas de	Se definieron indicadores los cuales permiten medir su efectividad y se cuenta con registros que permiten su trazabilidad.

Elementos	Comparación		
	Octubre 2014	Octubre 15	Observación
		indicadores	
8. Métricas	No se cuenta con métricas	Las 155 fichas de indicadores cuentan con las características requeridas para las métricas.	Se formularon las métricas para los indicadores definidos con sus respectivas metas.

Cuadro 4.13 Comparativa de situación de seguridad 2014 versus lo implementado.

c) Resultados de análisis costo beneficio de la implementación.

La implementación del modelo GSI-EGob en la Entidad de Control permite comparar el costo de los planes de tratamiento de riesgos identificados vs el impacto económico resultante de concretarse uno o todos los riesgos, para el cual se ha considerado el costo de las sanciones de incumplimiento de la Ley Nº 29733: Ley de protección de datos personales.

El cuadro 4.14, muestra el análisis costo beneficio (ver detalle en el Anexo G), en el que se observa que el costo total de la implementación de los controles es aproximadamente el 15% del costo del impacto de un riesgo de nivel medio, como el caso del riesgo 6.

Análisis Costo-Beneficio			
Plan de tratamiento del:	Costo de implementación de controles	Impacto del riesgo	Beneficio obtenido (Diferencia entre costo e impacto por riesgo)
Riesgo 1	S/. 37,280.00	S/. 22,725,500.00	S/. 22,688,220.00
Riesgo 2	S/. 176,640.00	S/. 22,725,500.00	S/. 22,548,860.00
Riesgo 3	S/.12,144.00	S/. 2,748,500.00	S/. 2,736,356.00
Riesgo 4	S/. 50,400.00	S/. 22,735,500.00	S/. 22,685,100.00
Riesgo 5	S/. 66,400.00	S/. 22,712,500.00	S/. 22,646,100.00
Riesgo 6	**S/. 18,440.00**	**S/. 2,736,500.00**	**S/. 2,718,060.00**
Riesgo 7	S/. 45,920.00	S/. 2,725,500.00	S/. 2,679,580.00
	S/. 407,224.00		

Cuadro 4.14 Comparativa de situación de seguridad 2014 versus lo implementado.

5 CAPITULO VI: CONCLUSIONES Y TRABAJOS FUTUROS

5.1. Conclusiones

Se elaboró un modelo de gestión de seguridad de la información para el gobierno electrónico resultado de la revisión y análisis de 11 modelos de seguridad de la información, en los que se identificaron los elementos más relevantes que forman parte del modelo propuesto.

Se ha definido una estructura organizacional con funciones definidas que contempla los procesos estratégicos, fundamentales y de soporte, la cual permite gestionar la seguridad de la información y garantizar una mejor experiencia al cliente cuando requiera interactuar con los procesos o servicios de la organización.

Se han identificado 05 niveles de madurez para la implementación y operación del modelo de seguridad de la información en los procesos que brindan servicio de gobierno electrónico, permitiendo la gestión de la seguridad en dichos procesos y conocer el nivel de seguridad con que se cuenta.

Se han establecido 114 controles de acuerdo a los niveles de madurez, iniciando con 30 en el nivel inicial (nivel 0) y finalizando con 114 en el nivel optimizado (nivel 5); asimismo se han establecido 10 documentos obligatorios para los 05 niveles.

Se han establecido 06 tipos de indicadores y métricas con sus respectivas características que permitan medir el desempeño de la gestión de seguridad en los servicios del gobierno electrónico.

Se propone una secuencia de 04 fases para la implementación del modelo en los proceso que brindan servicio de gobierno electrónico donde se explica los pasos a seguir, desde la planeación de la seguridad hasta su revisión y mejora del sistema de seguridad de la información implementado.

Este modelo dispone de un alto aporte en el cumplimiento de la NTP IEC/ISO 27001:2014 y el estándar ISM3, debido a que orienta y establece elementos necesarios para la implementación del sistema de gestión de seguridad de la información, siendo útil en la gestión de los procesos que brindan servicios de gobierno electrónico.

El modelo establece como parte de la implantación la realización de un análisis y evaluación de riesgos; el cual es muy importante en la toma de decisiones sobre los controles a implementar y su propósito de seguridad para reducir el impacto del riesgo a un nivel aceptable.

El modelo permite medir la seguridad global de los procesos que brindan servicio de gobierno electrónico en relación a los controles de seguridad con los que se cuenta, lo cual genera una tendencia hacia la mejora continua.

De la evaluación de los datos recopilados en la encuesta se ha observado que es importante orientan la seguridad de la información hacia los procesos fundamentales entre estos los que brindan servicio de gobierno electrónico. Asimismo los elementos que forman parte del modelo son considerados muy prioritarios.

5.2. Trabajos futuros.

Como trabajo futuro se sugiere considerar integrar los controles de acuerdo a lo requerido por la gestión de servicios de tecnologías de la información (ISO/IEC 20000) que soportan los procesos de servicios de gobierno electrónico que cuentan con seguridad de la información, integrados como una solución de inteligencia de negocios basados en indicadores y métricas.

El trabajo no cubre la posibilidad de agregar nuevos elementos en el caso que se vayan descubriendo nuevos requerimientos de seguridad en el entorno y que afecte los procesos de servicio electrónico. Se recomienda definir un nuevo modelo que asocie elementos para empresas con procesos 100% soportados en tecnologías de Cloud Computing.

Como trabajo futuro, un factor importante de la seguridad de la información es la gestión de los recursos humanos. Es posible que además de la organización y responsabilidades propuestas en el modelo del presente trabajo, sea necesario realizar un estudio para incluir otros elementos que intervengan directamente en la productividad del personal.

6 REFERENCIAS BIBLIOGRÁFICAS

[Almarabeh+ 2010] Almarabeh, T., & AbuAli, A. (2010). A General Framework for E-Government: Definition, Maturity Challenges, Opportunities, and Success. [versión electrónica] *European Journal of Scientific Research*, 39 (1) http://www.eurojournals.com/ejsr_39_1_03.pdf

[APDP, 2013] Autoridad Nacional de Protección de Datos Personales. Directiva de Seguridad de Seguridad de la Información, publicada en octubre de 2013, http://www.minjus.gob.pe/wp-content/.../Cartilla-de-Directiva-de-Seguridad.pdf

[Burgos+ 2011] Jorge Burgos y Pedro Campos. Modelo de Seguridad de la información en TIC, publicado por la Universidad del Bío-Bío en CEUR Workshop Proceedings - 2do Encuentro Informática y Gestión, Temuco, Chile, Noviembre 20-21, 2008.

[Chung-pin+2011] Chung-pin Lee, Kaiju Chang y Frances Stokes Berry. Testing the Development and Diffusion of E-Government and E-Democracy: A Global Perspective, Public Administration Review, June 2011

[Drucker 1999] Peter Drucker. Book: The new realities. Harper and Row, New York, 1989.

[Frohlich 2002] Frohlich,M.T. Techniques for improving response rates in OM survey research publicado por el Journal of Operations Management, 2002, 20, pp. 53–62.

[Gratton 2008] Gratton Lynda. Puntos calientes: Qué hace que algunos equipos vibren con energía y otros no; traductor Affán Buitrago. Bogota: Grupo editorial norma, 2008.

[ISO 2013] International Organization for Standardization. ISO IEC 27001:2013 EDI Tecnologías de la información. Técnicas de seguridad. Sistema de gestión de seguridad de la información. Requisitos, publicado en octubre de 2013, http:// http://www.iso.org/iso/home.htm

[Jiang+ 2000] Jiang James, Muhanna W y Klein G. User resistance and strategies for promoting acceptance across system types, Information & Management, v. 37, n. 1, 2000, pp. 25-36.

[Kamensky 1999] Kamensky, J. A Brief History. Consultado el 12 de mayo de 2011, página web de la Sociedad Nacional para la Reinvención del Gobierno del Vicepresidente Al Gore. http://govinfo.library.unt.edu/npr/whoweare/history2.html

[Karokola+ 2011] Geoffrey Karokola, Stewart Kowalski and Louise Yngström. Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View publicado por la universidad de stockolmo y el Instituto royal de tecnología en agosto de 2011.

[Mariño 2010] Alipio Mariño Obregón**.** Factores inhibidores en la implementación de sistemas de gestión de la seguridad de la información basados en la NTP-ISO/IEC 17799 en la administración pública. UNMSM-FISI 2010.

[MINTIC 2010] Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia. Modelo de seguridad de la información para la estrategia de gobierno en línea, publicado en diciembre de 2010. http://programa.gobiernoenlinea.gov.co/index.shtml

[OECD 2008] e-Government Studies. Future of e-government: Agenda 2020, OECD [version electrónica]. E-Leaders Conference 2008 Main Conclusions. http://www.oecd.org/dataoecd/41/40/43340370.pdf

[ONGEI 2010] Oficina Nacional de Gobierno Electrónico e Informática, Gobierno electrónico en el Perú, 2010

[Stallings 2007] William Stallings. The Internet Protocol Journal, Volume 10, No. 4, Dic 2007.

[The Open Group 2011] The Open Group. Open - Information Security management Maturity Model (O - ISM3) publicado en febrero de 2011.

[Thomas 2005] Thomas L. Friedman., The World Is Flat: A Brief History of the Twenty-first Century. Publicado por Farrar, Straus and Giroux en Abril de 2005.

[UNITED NATION 2008] United Nations Department of Economic and Social Affairs. United Nations E-Government Survey 2008: From E-Government to Connected Governance. http://www.un.org/desa, http://www.unpan.org/e-government

[UNITED NATION 2010] United Nations Department of Economic and Social Affairs. United Nations E-Government Survey 2010: Leveraging E-Government at a Time of Financial and Economic Crisis. http://www.un.org/desa, http://www.unpan.org/e-government

[UNITED NATION 2012] United Nations Department of Economic and Social Affairs. United Nations E-Government Survey 2012, E-Government for the People. http://www.un.org/desa, http://www.unpan.org/e-government

[UNITED NATION 2014] United Nations Department of Economic and Social Affairs. United Nations E-Government Survey 2014, Government for the Future We Want. http://www.un.org/desa, http://www.unpan.org/e-government

[Villegas+ 2009] Marianella Villegas, Orlando Viloria y Walter Blanco. Modelo de madurez de la seguridad de la información en el contexto de las organizaciones inteligentes, publicado en la 7ma conferencia de Latinoamérica y el caribe para ingeniería y tecnología (LACCEI'2009) en junio de 2009.

[Villegas+ 2011] Villegas Marianella, Meza Marina y León Pilar. Las métricas, elemento fundamental en la construcción de modelos de madurez de la seguridad informática, publicado en Redalyc (Red de revistas Científicas de América Latina, el Caribe, España y Portugal) – Universidad Rafael Belloso Chacín, Vol. XV, Núm. 1, enero-abril, 2011, pp.1-16.

[Viloria+ 2009] Viloria Orlando y Blanco Walter. Modelo sistémico de las seguridad de la información en las universidades, publicado en Redalyc (Red de revistas Científicas de América Latina, el Caribe, España y Portugal) – Universidad Central de Venezuela, Vol. XV, Núm. 1, enero-junio, 2009, pp.219-240.

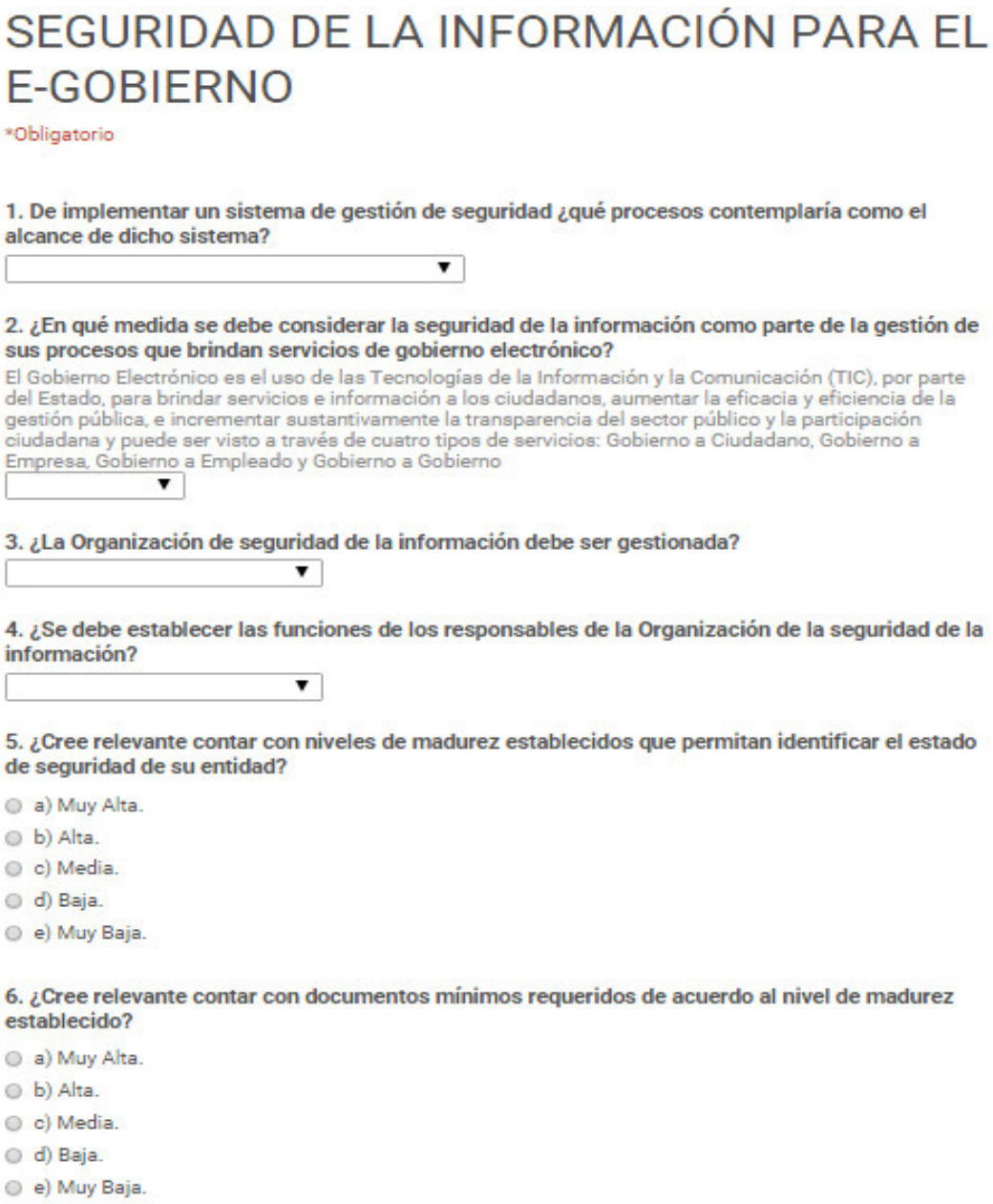
[Vladimir 2011] Vladimir Jirasek. Practical application of information security models, Technical Report, Volume 17, Issues 1–2, February 2012, Pages 1-8 publicado en ScienceDirect.
http://www.sciencedirect.com/science/article/pii/S1363412711000872

[West 2007] West, Darrell M. *Digital Government: Technology and Public Sector Performance*. Estados Unidos: Princeton University Press 2007.

ANEXO A
ENCUESTA: SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO

Encuesta elaborada través de las herramientas de Google (https://docs.google.com/forms/) y remitida vía email adjuntando los siguientes enlaces:

- Enlace normal: https://docs.google.com/forms/d/1gXG5xr_tfplpa6xvn8MO53aHNE0YtO3Af_t09tT856E/viewform
- Enlace corto : http://goo.gl/forms/gGPg6j36YQ



SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO

*Obligatorio

1. De implementar un sistema de gestión de seguridad ¿qué procesos contemplaría como el alcance de dicho sistema?

2. ¿En qué medida se debe considerar la seguridad de la información como parte de la gestión de sus procesos que brindan servicios de gobierno electrónico?

El Gobierno Electrónico es el uso de las Tecnologías de la Información y la Comunicación (TIC), por parte del Estado, para brindar servicios e información a los ciudadanos, aumentar la eficacia y eficiencia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación ciudadana y puede ser visto a través de cuatro tipos de servicios: Gobierno a Ciudadano, Gobierno a Empresa, Gobierno a Empleado y Gobierno a Gobierno

3. ¿La Organización de seguridad de la información debe ser gestionada?

4. ¿Se debe establecer las funciones de los responsables de la Organización de la seguridad de la información?

5. ¿Cree relevante contar con niveles de madurez establecidos que permitan identificar el estado de seguridad de su entidad?

- a) Muy Alta.
- b) Alta.
- c) Media.
- d) Baja.
- e) Muy Baja.

6. ¿Cree relevante contar con documentos mínimos requeridos de acuerdo al nivel de madurez establecido?

- a) Muy Alta.
- b) Alta.
- c) Media.
- d) Baja.
- e) Muy Baja.

7. ¿Cree relevante contar con controles mínimos requeridos de acuerdo al nivel de madurez establecido?

- a) Muy Alta.
- b) Alta.
- c) Media.
- d) Baja.
- e) Muy Baja.

8. ¿Cree relevante contar con indicadores que permitan monitorear los controles implementados de acuerdo a su propósito o finalidad?

- a) Muy Alta.
- b) Alta.
- c) Media.
- d) Baja.
- e) Muy Baja.

9. ¿Cree relevante contar con métricas que permitan conocer la viabilidad de los controles implementados de acuerdo a su propósito o finalidad?

- a) Muy Alta.
- b) Alta.
- c) Media.
- d) Baja.
- e) Muy Baja.

10. De contar con un modelo de gestión de seguridad de la información, ¿qué elementos cree que son más prioritarios para formar parte del modelo? *

	Muy prioritario	Medio prioritario	No es prioritario
Estructura organizacional para la gestión de la seguridad de la información.	○	○	○
Funciones de los responsables de la organización de la seguridad de la información.	○	○	○
Fases para la implementación y operatividad del sistema de seguridad.	○	○	○
Niveles de madurez del sistema de gestión de seguridad de la información.	○	○	○
Documentación requerida.	○	○	○
Controles de seguridad.	○	○	○
Indicadores alineados al propósito o finalidad de los controles.	○	○	○
Métricas que determinen la viabilidad de los indicadores.	○	○	○

10 (a) Respecto a la pregunta anterior, de considerar otro elemento, especifique el nombre del elemento y su prioridad.

(Donde: 1 es muy prioritario, 2 es medio prioritario y 3 no es prioritario).

Si desea se le remita los documentos indicados, por favor brindar su cuenta de correo

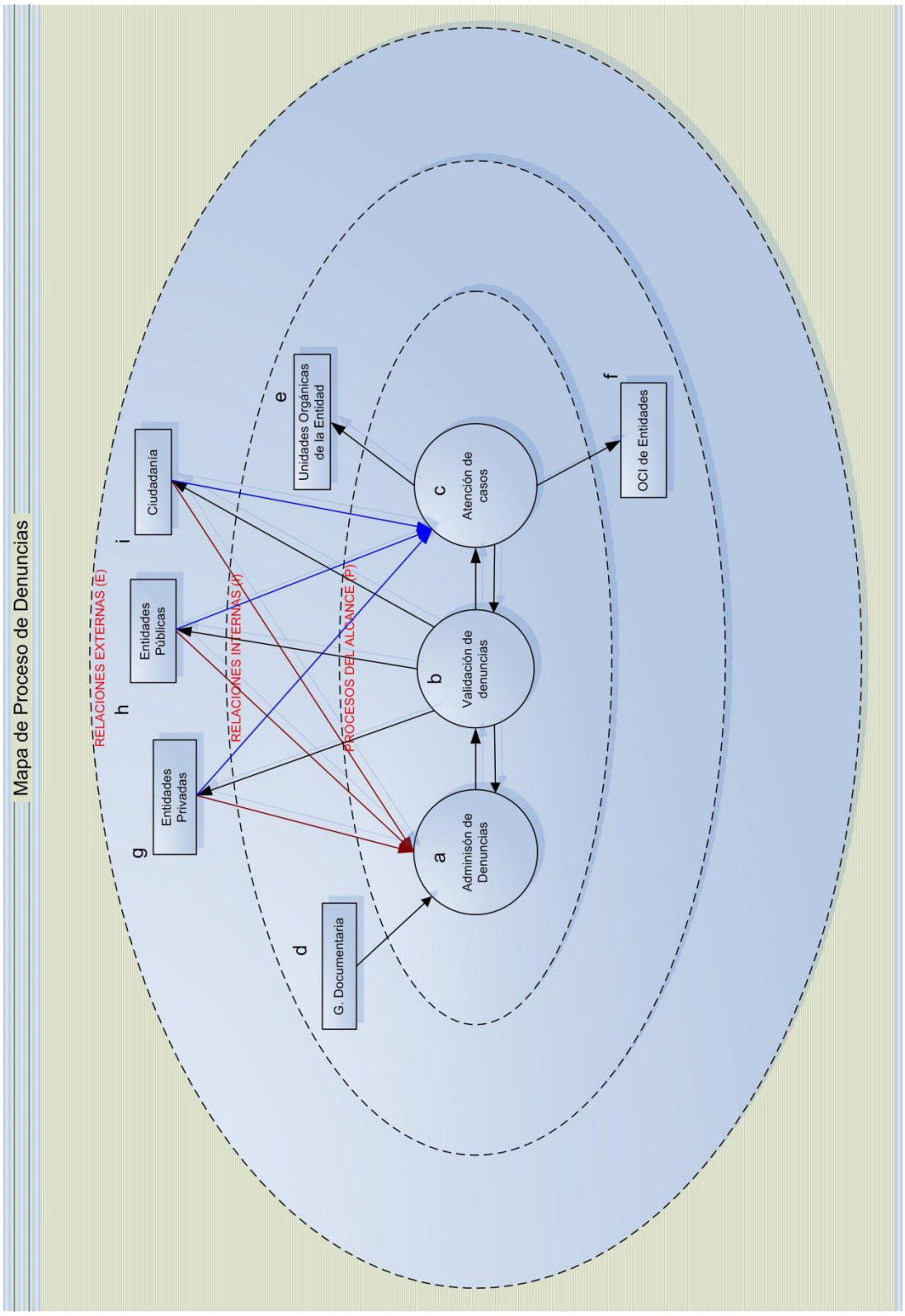
Metodología de Gestión de Riesgos de seguridad de la Información / Matriz de modelo de seguridad de la información por niveles de madurez

Enviar

Nunca envíes contraseñas a través de Formularios de Google.

ANEXO B

DIAGRAMA CONTEXTUAL DEL PROCESO DE DENUNCIAS



ANEXO C

GESTIÓN DE RIESGOS: INVENTARIO DE ACTIVOS DE INFORMACIÓN

Nº.	Activo de Información	Categoría	Sub-categoría	Tipo	Ubicación física o lógica	Unidad orgánica		
						Propietario	Usuario	Custodio
1	Analista de recepción y admisión	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
2	Analista de organización de casos	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
3	Gestor de atención al ciudadano	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
4	supervisor general	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
5	supervisor de equipo	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
6	operador documentario	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
7	gerente de departamento	AP	PS	PF	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
8	Aplicativo G. Denuncia	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC
9	Sistema Documentario	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC
10	Sistema Trámite expedientes	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC
11	Correo	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC
12	Intranet	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC
13	Registro de atención a ciudadano	PM	IF	RA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
14	formulario para presentar denuncia	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
15	compromiso del denunciante	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
16	Formulario web	PM	IE	RA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
17	Formato cero	PM	IF	RA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
18	Oficio de respuesta a consulta de ciudadano	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
19	Oficio de procedencia de solicitud de protección	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
20	Oficio de confirmación de trámite ciudadano	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
21	Oficio de derivación de la denuncia - entidad competente	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
22	Oficio de derivación su denuncia - ciudadano	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
23	Formato caso	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
24	Oficio de requerimiento de información adicional	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
25	Información adicional requerida	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
26	Oficio de acreditación	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
27	Memorando de derivación de la denuncia a la U.O	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
28	Oficio de derivación de la denuncia al OCI	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
29	Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad	PM	IF	DA	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
30	Oficio de denuncia desestimada - Ciudadano	PM	IF	DC	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
31	Computadora de Analista de recepción y admisión	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
32	Computadora de Analista de organización de casos	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
33	Computadora de Gestor de atención al ciudadano	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
34	Computadora de supervisor general	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
35	Computadora de supervisor de equipo	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
36	Computadora de operador documentario	AP	HW	DT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
37	Computadora de gerente de departamento	AP	HW	LT	Sede Central	DENUNCIA	DENUNCIA	DENUNCIA
38	Aplicativo SED	AP	SW	SA	Sede Central	DENUNCIA	DENUNCIA	TIC

ANEXO D

GESTIÓN DE RIESGOS: VALORIZACIÓN DE ACTIVOS

ACTIVOS Cuánto afecta la pérdida, manipulación o deterioro del activo (Y) a los criterios de evaluacion (X)		Criterios																					VALORIZACION DEL ACTIVO (Impacto)
		CONFIDENCIAL			INTEGRIDAD			DISPONIBIL.			NO-REPUDIO			AUTENTICIDAD			CONFIABILIDAD			RENDICION DE CUENTAS			
N°	Nombre del activo	ACCESO A LA INFORMACIÓN NO PÚBLICA	DIVULGACIÓN DE LA INFORMACIÓN PRIVADA O RESTRINGIDA	RUPTURA EN LOS MECANISMOS SEGURIDAD	INCONSISTENCIA DE LA INFORMACIÓN O DATOS	PÉRDIDA DE INFORMACIÓN O DATOS	REDUNDANCIA DE DATOS O INFORMACIÓN	RETRASO EN LA ENTREGA DE LA INFORMACIÓN	INEXISTENCIA DE INFORMACIÓN	INFORMACIÓN DESACTUALIZADA	INSEGURIDAD EN LAS TRANSMISIONES DE INFORMACIÓN O DATOS	NO ACEPTACION DE LA TRANSMISION DE INFORMACIÓN O DATOS	INTERRUPCIÓN DE LAS COMUNICACIONES	INFRACCIÓN DE LAS LEYES O REGULACIONES	PÉRDIDA DEL VALOR LEGAL DE LA INFORMACIÓN	SUPLANTACION DEL ORIGINAL	INVALIDEZ DE LA INFORMACIÓN O DATOS	PÉRDIDA DE BUENA IMAGEN INSTITUCIONAL	INTERRUPCIÓN EN LAS OPERACIONES DE TERCEROS O INTERNAS	COSTO DE REEMPLAZO	COSTO INTERNO ADICIONAL DE OTROS ACTIVOS, SERVICIOS O	COSTO DE MANTENIMIENTO	
1	Analista de recepción y adminsión	3	4	3	4	4	4	1	5	2	1	1	1	3	5	5	4	5	4	2	2	2	2.95
2	Analista de organización de casos	4	4	3	4	4	4	1	5	1	2	2	2	4	4	4	4	4	3	4	3	4	3.33
3	Gestor de atención al ciudadano	2	2	3	4	4	4	2	2	1	2	1	2	2	2	5	3	5	5	3	2	3	2.81
4	supervisor general	3	3	4	4	4	3	3	3	3	1	1	1	3	4	3	4	3	3	3	3	3	2.95
5	supervisor de equipo	5	5	5	5	5	5	3	3	3	1	1	1	5	5	5	5	3	4	5	3	4	3.86
6	operador documentario	5	5	5	4	4	5	5	4	4	4	3	2	2	1	1	3	1	2	1	1	1	3.00
7	gerente de departamento	5	5	5	5	4	5	5	5	5	4	4	2	2	1	1	4	1	3	1	1	1	3.29
8	Aplicativo G. Denuncia	5	5	5	5	4	5	5	5	5	5	5	4	3	2	3	5	2	4	3	3	3	4.10
9	Sistema Documentario	3	2	2	3	3	3	1	1	1	3	3	3	2	2	2	3	2	4	3	4	3	2.52
10	Sistema Trámite expedientes	5	5	5	5	5	5	4	4	4	5	5	5	2	5	5	5	3	5	5	5	5	4.62
11	Correo	2	2	3	2	1	2	1	1	1	2	2	2	2	2	1	2	2	2	2	1	1	1.71
12	Intranet	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1.10
13	Registro de atención a ciudadano	2	2	4	3	4	3	4	4	4	2	2	3	2	2	2	5	1	2	1	2	1	2.62
14	formulario para presentar denuncia	4	5	5	1	1	2	1	1	1	3	2	1	1	1	1	5	1	3	1	5	1	2.19
15	compromiso del denunciante	1	1	5	1	2	1	1	1	1	1	2	1	1	1	1	3	1	1	1	1	1	1.38
16	Formulario web	3	4	5	3	2	2	2	3	1	5	5	4	3	2	2	5	1	2	2	4	3	3.00
17	Formato cero	3	3	5	1	2	2	4	4	5	2	2	1	1	1	1	4	1	1	1	1	1	2.19
18	Oficio de respuesta a consulta de ciudadano	2	1	4	1	1	2	4	4	4	1	1	1	1	1	4	2	2	2	1	1	1	1.95
19	Oficio de procedencia de solicitud de protección	2	1	4	1	1	2	4	4	4	1	1	1	1	1	2	2	2	2	1	1	1	1.86
20	Oficio de confirmación de trámite ciudadano	2	1	4	1	1	1	4	4	4	1	1	1	1	1	2	2	2	2	1	1	1	1.81
21	Oficio de derivación de la denuncia - entidad competente	2	1	4	1	1	1	3	3	3	1	1	1	1	1	1	2	2	4	1	1	1	1.71
22	Oficio de derivación su denuncia - ciudadano	2	1	4	1	1	1	3	3	3	1	1	1	1	1	1	2	2	3	1	1	1	1.67
23	Formato caso	5	5	5	4	4	3	3	3	3	1	5	2	5	2	2	2	1	3	1	1	1	2.90
24	Oficio de requerimiento de información adicional	2	3	3	1	1	2	3	3	3	3	3	2	2	2	2	3	2	1	2	2	2	2.24
25	Información adicional requerida	4	5	5	1	1	2	3	3	3	3	3	2	2	2	2	3	2	1	2	2	2	2.52
26	Oficio de acreditación	1	1	3	1	1	1	1	1	1	1	1	1	1	4	1	1	2	2	1	1	1	1.33
27	Memorando de derivación de la denuncia a la U.O	2	3	1	1	1	2	1	1	2	1	1	1	1	1	1	2	2	2	1	1	1	1.38
28	Oficio de derivación de la denuncia al OCI	2	3	3	2	2	1	2	1	1	2	2	2	1	1	1	2	2	2	1	1	1	1.52
29	Oficio de solicitud de información sobre adopcion de medidas correctivas - Entidad	2	3	1	2	1	1	3	1	2	1	2	2	1	1	1	2	2	2	1	1	1	1.57
30	Oficio de denuncia desestimada - Ciudadano	2	3	1	1	1	1	1	1	1	2	2	2	1	2	1	1	1	1	1	1	1	1.33
31	Computadora de Analista de recepción y adminsión	5	3	5	3	4	2	4	3	3	4	3	2	1	2	1	2	1	2	1	1	1	2.52
32	Computadora de Analista de organización de casos	5	4	5	3	5	1	4	4	4	4	2	2	1	1	1	3	1	2	1	1	1	2.62
33	Computadora de Gestor de atención al ciudadano	4	5	4	4	2	4	3	5	4	2	4	4	1	3	2	3	2	3	2	2	2	3.10
34	Computadora de supervisor general	5	5	5	4	4	4	5	4	3	4	3	2	2	2	2	3	2	2	1	2	1	3.10
35	Computadora de supervisor de equipo	5	5	5	5	5	5	5	5	5	1	1	1	5	5	5	5	5	5	5	5	2	4.29
36	Computadora de operador documentario	5	5	5	5	4	5	5	5	5	4	4	2	2	1	1	4	1	3	1	1	1	3.29
37	Computadora de gerente de departamento	5	5	5	5	4	5	5	5	5	5	5	2	3	2	2	5	2	4	1	1	1	3.67
38	Aplicativo SED	5	5	5	5	4	5	5	5	5	5	5	4	3	2	2	5	2	4	2	3	3	4.00

ANEXO E

GESTIÓN DE RIESGOS: ANÁLISIS DE RIESGOS

N°	ACTIVOS: Riesgos	ACTIVOS: Nombre del Activo	ACTIVOS: Impacto del activo (a)	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA: AMENAZA: Fuente de Amenaza	AMENAZA: Descripción de la Amenaza	AMENAZA: Probabilidad de ocurrencia de la amenaza (b)	VULNERABILIDAD: Control existente	VULNERABILIDAD: Descripcion de la Vulnerabilidad	VULNERABILIDAD: Nivel de vulnerabilidad (c)	Probabilidad de ocurrencia de que la amenaza explote la vulnerabilidad (d)=(b*c)	Mayor valor de la probabilidad de ocurrencia (de que la amenaza explote la vulnerabilidad) del riesgo (e)	Valor o nivel del riesgo del activo (f)=(a*e)	Priorización de Activos
01	Publicación de identidad de denunciante y contenido de denuncia física recepcionada por la Entidad.	Formulario para presentar denuncia	2.62	Terceros	Dar a conocer la identidad del denuncia	1	No	No se diferencia denuncia original de cargo	4	4	4	10.47619048	Bajo
		Registro de atención a ciudadano	2.19					La denuncia y datos del denunciante no se registran en documentos separados.	4	4		8.761904762	Aceptable
02	Obtener de la web datos de denunciante y contenido de denuncia de la computadora usada por el denunciante.	Formulario web	3	Terceros	Obtener la denuncia y denunciante desde la computadora usada	5	Protocolo https	Almacenamiento temporal de la web no es eliminado / no utiliza un protocolo seguro (https)	4	20	20	60	Alto
03	Divulgar identidad de denunciante y contenido de denuncia desde el Sist. G. Denuncia o físico.	Aplicativo G. Denuncias (web)	4	Trabajador	Obtener la denuncia y denunciante desde el Sist. G. Denuncia/ Sist. Trámite expediente / aplicativos	5	Administración de Usuario y Password	Derivación de denuncias con datos del denunciante a los diferentes actores hasta el evaluador final (APA) a través de los sistemas.	3	15	20	80	Alto
		Sist. G. Documentario.	2.523810					No se realiza la revisión periodica de acuerdos de confidencialidad y accesos	4	20		50.47619048	Alto
		Aplicativo SED	4									80	Alto
		Sist. Trámite Expedientes	4.619048									92.38095238	Muy Alto
		Formulario web	3							0		60	Alto
		Registro de atención a ciudadano	2.19							0		43.80952381	Medio
		Formulario para presentar denuncia	2.190476	Trabajador	Obtener la denuncia y denunciante desde el físico y Sist. G. Denuncia	4	No	No se realiza la revisión periodica de acuerdos de confidencialidad y accesos	4	16	20	43.80952381	Medio
		Formato oficio	2.190476					La denuncia y datos del denunciante no se registran en documentos separados.	3	12		43.80952381	Medio
		Formato cargo	2.904762							0		58.09523810	Alto
		Compromiso del denunciante	1.380952							0		27.61904762	Medio
		Oficio de derivación de la denuncia al OCI	1.523810							0		30.47619048	Medio
		Computadora de Analista de recepción y admision	2.523810	Personal de U.O	Infectar con virus	2	Antivirus	Abrir correos desconocidos y descargar archivos o acceder a links contenidos en estos	3	6		40.38095238	Medio
		Computadora de Analista de organización de casos	2.619048					Ingresar USB infectados	3	6		41.90476190	Medio
		Computadora de Gestor de atención al ciudadano	3.095238									49.52380952	Alto
		Computadora de Analista de recepción y admision	2.523810					Detener o cancelar los procedimientos de actualización durante su ejecución	3	12		40.38095238	Medio
		Computadora de Analista de organización de casos	2.619048					Personal no cuenta con el conocimiento o capacitacion en procedimientos alternos y adecuado uso de equipos	4	16		41.90476190	Medio

ACTIVOS				PROBABILIDAD DE OCURRENCIA DE LA AMENAZA								
				AMENAZA				VULNERABILIDAD				
N°	Riesgos	Nombre del Activo	Impacto del activo (a)	Fuente de Amenaza	Descripción de la Amenaza	Probabilidad de ocurrencia de la amenaza (b)	Control existente	Descripcion de la Vulnerabilidad	Nivel de vulnerabilidad (c)	Probabilidad de ocurrencia de que la amenaza explote la vulnerabilidad (d)=(b*c)	Mayor valor de la probabilidad de ocurrencia (de que la amenaza explote la vulnerabilidad) del riesgo (e)	Valor o nivel del riesgo del activo (f)=(a*e)	Priorización de Activos
4	No se puede atender oportunamente la denuncia recibida,	Computadora de Gestor de atención al ciudadano	3.095238	Personal de U.O	Ocasionar falla en equipos o Aplicativos	4	No	No se cuenta con procedimientos alternos y adecuado uso de equipos	4	16	16	49.5238095	Alto
		Computadora de supervisor general	3.095238									49.5238095	Alto
		Computadora de supervisor de equipo	4.285714									68.5714286	Alto
		Computadora de operador documentario	3.285714									52.5714286	Alto
		Computadora de gerente de departamento	3.666667									58.6666667	Alto
		Aplicativo G. Denuncias (web)	4									64	Alto
		Sist. G. Documentario.	2.52381									40.3809524	Medio
		Sist. Trámite Expedientes	4.619048									73.9047619	Alto
		Computadora de Analista de recepción y admisión	2.52381	Personal de DTI / DING / U.O	Ocasionar caida de circuito de red o eléctrico	1	No	Manipulación de la red por personal de soporte.	2	2		40.3809524	Medio
		Computadora de Analista de organización de casos	2.619048	Servicio de Luz	Ocasionar caida de servicio eléctrico	1		Equipo eléctrico de cómputo y electrodomésticos en un mismo circuito.	3	3		41.9047619	Medio
		Computadora de Gestor de atención al ciudadano	3.095238					Mantenimiento de circuito de red en horarios de oficina	1	1		49.5238095	Alto
		Computadora de supervisor general	3.095238					No se cuenta con procedimientos alternos o de respaldo para la continuidad de las operaciones	3	3		49.5238095	Alto
		Computadora de supervisor de equipo	4.285714									68.5714286	Alto
		Computadora de operador documentario	3.285714									52.5714286	Alto
		Computadora de gerente de departamento	3.666667									58.6666667	Alto
		Aplicativo G. Denuncias (web)	4									64	Alto
		Sist. G. Documentario.	2.52381									40.3809524	Medio
		Sist. Trámite Expedientes	4.619048									73.9047619	Alto
5	Perdida o extravio de documento de denuncia	Formulario para presentar denuncia	2.190476	Trabajador	No cumplir con los procedimientos establecidos	2	No	Falta control de los documentos en recepción, digitalización y derivación	3	6	6	13.1428571	Bajo
		Formato cero	2.190476									13.1428571	Bajo
		Formato caso	2.904762									17.4285714	Bajo
		Información adicional requerida	2.52381									15.1428571	Bajo
		Compromiso del denunciante	1.380952									8.28571429	Aceptable
		Registro de atención a ciudadano	2.19									13.1428571	Bajo

ACTIVOS				PROBABILIDAD DE OCURRENCIA DE LA AMENAZA								
				AMENAZA				VULNERABILIDAD				
N°	Riesgos	Nombre del Activo	Impacto del activo (a)	Fuente de Amenaza	Descripción de la Amenaza	Probabilidad de ocurrencia de la amenaza (b)	Control existente	Descripcion de la Vulnerabilidad	Nivel de vulnerabilidad (c)	Probabilidad de ocurrencia de que la amenaza explote la vulnerabilidad (d)=(b*c)	Mayor valor de la probabilidad de ocurrencia (de que la amenaza explote la vulnerabilidad) del riesgo (e)	Valor o nivel del riesgo del activo (f)=(a*e)	Priorización de Activos
6	Divulgar Identidad de denunciante, contenido de denuncia y evaluación de documento de resolución	Oficio de respuesta a consulta de ciudadano	1.952381	Tercero	Obtener la denuncia, datos de denunciante y evaluación.	4	No	mensajeria entrega oficios a pernosas no autorizadas.	4	16	16	31.2380952	Medio
		Oficio de derivación de la denuncia - entidad competente	1.714286	Mensajero	Vende información de la denuncia, datos de denunciante y evaluación.	4		Sobre con oficios no es seguro	4	16		27.4285714	Medio
		Oficio de derivación de su denuncia - ciudadano	1.666667					Procedimiento de mensajeria no contempla medidas de confidencialidad.	3	12		26.6666667	Medio
		Formato caso	2.904762									46.4761905	Alto
		Memorando de derivación de la denuncia a la U.O	1.380952									22.0952381	Medio
		Oficio de derivación de la denuncia al OCI	1.52381									24.3809524	Medio
		Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad	1.571429									25.1428571	Medio
		Oficio de denuncia desestimada - Ciudadano	1.333333									21.3333333	Medio
7	Emitir Oficio de respuesta con Pronunciamiento incorrecto	Formato caso	2.904762	Personal analista	No cumplir con los procedimientos establecidos	1	No	Sistema Informático (Sist. G. Denuncia) no permite realizar la trazabilidad del procedimiento de evaluación de denuncias.	3	3	12	34.8571429	Medio
		Registro de atención a ciudadano	2.19	Denunciado	Entrega información no veridica.	2		No se valida in situ la información remitida de ser necesario.	3	6		26.2857143	Medio
		Información adicional requerida	2.52381	Denunciado	Omite o no entrega información	2		No se cuenta con la operacionalización del RIS	2	4		30.2857143	Medio
8	Información procesada (denuncia en evaluación) es accedida por diferentes U.O sin control.	Aplicativo G. Denuncias (web)	4	Personal de otras U.O	Accede a información de la denuncia en evaluación	4	No	No se establecen criterios para resguardarla confidencialidad de la denuncia en las consultas a BD.	3	12	12	48	Alto
		Aplicativo SED	4									48	Alto
		Sist. G. Documentario.	2.52381									30.2857143	Medio
		Sist. Trámite Expedientes	4.619048									55.4285714	Alto

ANEXO F

GESTIÓN DE RIESGOS: EVALUACIÓN DE RIESGOS

N°	Riesgo	Activos de Información	Amenazas	Criterios de Impacto del riesgo en el negocio					Impacto del riesgo en el negocio (g)	Mayor valor de Impacto de riesgo por activo (h)	Mayor valor de probabilidad de ocurrencia del riesgo (e)	Valor del riesgo en el negocio (f=e*h)	
				Impacto económico del riesgo	Buena Imagen y prestigio	Requisitos contractuales legales y regulatorios	Probabilidad de Interrumpir las actividades u operaciones	Tiempo de recuperación de las operaciones					
1	Publicación de identidad de denunciante y contenido de denuncia física recepcionada por la Entidad.	Formulario para presentar denuncia	Dar a conocer la identidad del denuncia	2	4	4	1	1	2.4	2.4	4	9.6	Aceptable
		Registro de atención a ciudadano		2	4	4	1	1	2.4				
2	Obtener de la web datos de denunciante y contenido de denuncia de la computadora udata por el denunciante	Formulario web	Obtener la denuncia y denunciante desde la computadora usada	3	5	5	2	2	3.4	3.4	20	68	Alto
3	Divulgar identidad de denunciante y contenido de denuncia desde el Sist. G. Denuncias o físico.	Aplicativo G. Denuncia (Web)	Obtener la denuncia y denunciante desde el Sist. G. Denuncias / Sist. Trámite Expediente / aplicativos	3	5	4	2	2	3.2	3.2	20	64	Alto
		Sist. Documentario		1	1	1	1	1	1				
		Aplicativo SED		1	3	3	1	1	1.8				
		Sist. Trámite Expediente.		1	4	4	1	1	2.2				
		Formulario web		2	5	5	1	1	2.8				
		Registro de atención a ciudadano		2	5	5	1	1	2.8				
		Formulario para presentar denuncia	Obtener la denuncia y denunciante desde el físico y Sist. G. Denuncias	2	5	5	1	1	2.8				
		Formato cero		1	1	1	1	1	1				
		Formato caso		2	5	5	1	1	2.8				
		Compromiso del denunciante		2	5	5	1	1	2.8				
		Oficio de derivación de la denuncia al OCI		2	5	5	1	1	2.8				
4	No se puede atender oportunamente la denuncia recibida.	Computadora de Analista de recepción y admisión	Infectar con virus	2	1	1	2	1	1.4	1.4	16	22.4	Medio
		Computadora de Analista de organización de casos		2	1	1	2	1	1.4				
		Computadora de Gestor de atención al ciudadano		2	1	1	2	1	1.4				
		Computadora de Analista de recepción y admisión	Ocasionar falla en equipos o Aplicativos	2	3	3	2	1	2.2				
		Computadora de Analista de organización de casos		2	3	3	2	1	2.2				
		Computadora de Gestor de atención al ciudadano		2	3	3	2	1	2.2				
		Computadora de supervisor general		2	3	3	1	1	2				
		Computadora de supervisor de equipo		2	3	3	1	1	2				
		Computadora de operador documentario		2	3	3	2	1	2.2				
		Computadora de gerente de departamento		2	3	3	1	1	2				
		Aplicativo G. Denuncia (Web)		3	3	3	3	3	3				
		Sist. Documentario		3	3	3	2	2	2.6				
		Sist. Trámite Expediente.		3	3	3	2	2	2.6				
		Computadora de Analista de recepción y admisión	Ocasionar pérdida de	2	3	3	2	1	2.2				
		Computadora de Analista de organización de casos		2	3	3	2	1	2.2				
		Computadora de Gestor de atención al ciudadano		2	3	3	2	1	2.2				
		Computadora de supervisor general		2	3	3	1	1	2				

N°	Riesgo	Activos de información	Amenazas	Criterios de impacto del riesgo en el negocio					Impacto del riesgo en el negocio (g)	Mayor valor de impacto de riesgo por activo (h)	Mayor valor de probabilidad de ocurrencia del riesgo (e)	Valor del riesgo en el negocio (i=e*h)	
				Impacto económico del riesgo	Buena imagen y prestigio	Requisitos contractuales legales y regulatorios	Probabilidad de interrumpir las actividades u operaciones	Tiempo de recuperación de las operaciones					
		Computadora de supervisor de equipo	Ocasionar caída de circuito de red o eléctrico	2	3	3	1	1	2				
		Computadora de operador documentario		2	3	3	2	1	2.2				
		Computadora de gerente de departamento		2	3	3	1	1	2				
		Aplicativo G. Denuncia (Web)		3	3	3	3	3	3				
		Sist. Documentario		3	3	3	2	2	2.6				
		Sist. Trámite Expediente.		3	3	3	2	2	2.6				
		Computadora de Analista de recepción y admisión	Ocasionar caída de servicio eléctrico	2	3	3	2	1	2.2				
		Computadora de Analista de organización de casos		2	3	3	2	1	2.2				
		Computadora de Gestor de atención al ciudadano		2	3	3	2	1	2.2				
		Computadora de supervisor general		2	3	3	1	1	2				
		Computadora de supervisor de equipo		2	3	3	1	1	2				
		Computadora de operador documentario		2	3	3	2	1	2.2				
		Computadora de gerente de departamento		2	3	3	1	1	2				
		Aplicativo G. Denuncia (Web)		3	3	3	3	3	3				
		Sist. Documentario		3	3	3	2	2	2.6				
		Sist. Trámite Expediente.		3	3	3	2	2	2.6				
5	Perdida o extravío de documento de denuncia	Formulario para presentar denuncia	No cumplir con los procedimientos establecidos	3	3	5	3	3	3.4	3.4	6	20.4	Medio
		Formato cero		2	3	2	1	1	1.8				
		Formato caso		2	3	2	1	1	1.8				
		Información adicional requerida		2	3	2	1	1	1.8				
		Compromiso del denunciante		2	3	5	3	3	3.2				
		Registro de atención a ciudadano		3	3	5	3	3	3.4				
		Oficio de respuesta a consulta de ciudadano	Obtener la denuncia, datos de denunciante y evaluación.	1	4	4	1	1	2.2				
		Oficio de derivación de la denuncia - entidad competente		1	4	4	1	1	2.2				
		Oficio de derivación de su denuncia - ciudadano		1	4	4	1	1	2.2				
		Formato caso		1	4	4	1	1	2.2				
		Memorando de derivación de la denuncia a la U.O		1	4	4	1	1	2.2				
		Oficio de derivación de la denuncia al OCI		1	4	4	1	1	2.2				
		Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad		1	4	4	1	1	2.2				
6	Divulgar identidad de denunciante, contenido de denuncia y evaluación de	Oficio de denuncia desestimada - Ciudadano		1	4	4	1	1	2.2	2.2	16	35.2	Medio

Nº	Riesgo	Activos de información	Amenazas	Criterios de impacto del riesgo en el negocio					Impacto del riesgo en el negocio (g)	Mayor valor de impacto de riesgo por activo (h)	Mayor valor de probabilidad de ocurrencia del riesgo (e)	Valor del riesgo en el negocio (I=e*h)	
				Impacto económico del riesgo	Buena imagen y prestigio	Requisitos contractuales legales y regulatorios	Probabilidad de interrumpir las actividades u operaciones	Tiempo de recuperación de las operaciones					
[illegible]	[illegible] documento de resolución durante el envío.	Oficio de respuesta a consulta de ciudadano	Vende información de la denuncia, datos de denunciante y evaluación.	1	4	4	1	1	2.2	[illegible]	[illegible]	[illegible]	[illegible]
		Oficio de derivación de la denuncia - entidad competente		1	4	4	1	1	2.2				
		Oficio de derivación de su denuncia - ciudadano		1	4	4	1	1	2.2				
		Formato caso		1	4	4	1	1	2.2				
		Memorando de derivación de la denuncia a la U.O		1	4	4	1	1	2.2				
		Oficio de derivación de la denuncia al OCI		1	4	4	1	1	2.2				
		Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad		1	4	4	1	1	2.2				
		Oficio de denuncia desestimada - Ciudadano		1	4	4	1	1	2.2				
7	Emitir Oficio de respuesta con Pronunciamiento incorrecto	Formato caso	No cumplir con los procedimientos establecidos	4	3	4	2	2	3	3	12	36	Medio
		Registro de atención a ciudadano		4	3	4	2	2	3				
		Información adicional requerida		2	2	4	2	2	2.4				
		Formato caso	Entrega información no verídica.	4	3	4	2	2	3				
		Registro de atención a ciudadano		4	3	4	2	2	3				
		Información adicional requerida		4	3	4	2	2	3				
		Formato caso	Omite o no entrega información	4	3	4	2	2	3				
		Registro de atención a ciudadano		4	3	4	2	2	3				
		Información adicional requerida		4	3	4	2	2	3				
8	Información procesada (denuncia en evaluación) es accedida por diferentes U.O sin control.	Aplicativo G. Denuncia (Web)	Accede a información de la denuncia en evaluación	2	2	2	2	2	2	2	12	24	Medio
		Aplicativo SED		2	2	2	2	2	2				
		Sist. Documentario		2	2	2	2	2	2				
		Sist. Trámite Expediente.		2	2	2	2	2	2				

ANEXO G

GESTIÓN DE RIESGOS: PLAN DE TRATAMIENTO DEL RIESGO

Nº	Riesgo	Activos de Información	Amenazas	Valor del riesgo en el negocio	Priorización	Tratamiento del Riesgo				Riesgo Residual			
						Control Existente	Opción de tratamiento	Detalle de control a realizar	Periodo	Responsable de implementar controles	Probabilidad de ocurrencia del riesgo	Impacto del riesgo en el negocio	Valor del riesgo en el negocio
1	Obtener de la web datos de denunciante y contenido de denuncia de la computadora usada por el denunciante	Formulario web	Obtener la denuncia y denunciante desde la computadora usada	68	Alto	Protocolo https	Evitar	Implementar la eliminación de datos temporales de formulario web. Limpiar formularios al cerrar sesión.	2 meses	DENUNCIAS / TIC	2.4	4	9.6	Aceptable
2	Divulgar identidad de denunciante y contenido de denuncia desde el G. Denuncias o físico.	Aplicativo G. Denuncias Sist. Documentario Aplicativo SED SICGR - Trámite documentario Formulario web Registro de atención a ciudadano	Obtener la denuncia y denunciante desde el G. Denuncias / SICGR / aplicativos	64	Alto	Administración de Usuario y Password	Mitigar	Revisión y bloqueo de usuarios que no han sido autorizados por el DENUNCIAS	3 meses	Acceso solo a los usuarios autorizados expresamente por DENUNCIAS y solo a la información que no es confidencial	3.2	3	9.6	Aceptable
		Formulario para presentar denuncia Formato oficio Formato caso Compromiso del denunciante Oficio de derivación de la denuncia al OCI	Obtener la denuncia y denunciante desde el físico y G. Denuncias			No	Mitigar	> Revisión y bloqueo de usuarios que no han sido autorizados por el DENUNCIAS > Restringir el acceso a los expedientes de denuncias. > Encriptar la información de los denunciantes en las Bases de Datos que lo contengan. >Implemetar en G. Denuncias la trasabilidad de acceso a información de denuncias.	6 meses	DENUNCIAS / TIC				
3	No se puede atender oportunamente la denuncia recibida,	Computadora de Analista de recepción y admisión Computadora de Analista de organización de casos Computadora de Gestor de atención al ciudadano Computadora de supervisor general	Infectar con virus	22.4	Medio	Antivirus	Mitigar	Actualizar antivirus y bloquear archivos con extensiones ejecutables	2 semanas	TIC	1.4	4	5.6	Aceptable
		Computadora de Analista de recepción y admisión Computadora de Analista de organización de casos Computadora de Gestor de atención al ciudadano Computadora de supervisor general Computadora de supervisor de equipo Computadora de operador documentario Computadora de gerente de departamento	Ocasionar falla en equipos o Aplicativos			No	Mitigar	Establecer políticas de uso y configuración de equipos.	3 meses	TIC				
		Aplicativo G. Denuncias Sist. Documentario SICGR - Trámite documentario Computadora de Analista de recepción y admisión Computadora de Analista de organización de casos Computadora de Gestor de atención al ciudadano Computadora de supervisor general	Ocasionar salida de					> Comunicar al personal las medidas de seguridad respecto a los tipos de equipos electricos a utilizar de acuerdo al nivel de						

N°	Riesgo	Activos de información	Amenazas	Valor del riesgo en el negocio	Priorización	Tratamiento del Riesgo					Riesgo Residual			
						Control Existente	Opción de tratamiento	Detalle de control a realizar	Periodo	Responsable de implementar controles	Probabilidad de ocurrencia del riesgo	Impacto del riesgo en el negocio	Valor del riesgo en el negocio (I=e*h)	
		Computadora de supervisor de equipo Computadora de operador documentario Computadora de gerente de departamento Aplicativo G. Denuncias Sist. Documentario SICGR - Trámite documentario	Ocasional caída de circuito de red o eléctrico			No	Mitigar	voltios y amperios soportado por el circuito eléctrico. > Comunicar al personal los horarios de mantenimiento y reparaciones fuera de horario de oficina.	2 semanas	LOGÍSTICA				
4	Perdida o extravio de documento de denuncia	Formulario para presentar denuncia Formato cero Formato caso Información adicional requerida Compromiso del denunciante Registro de atención a ciudadano	No cumplir con los procedimientos establecidos	20.4	Medio	No	Mitigar	Establecer controles de seguimiento documental en los procedimientos de recepción, digitalización y derivación de documentos	3 meses	DENUNCIAS	2.4	2	4.8	Aceptable
5	Divulgar identidad de denunciante, contenido de denuncia y evaluación de documento de resolución durante el envio.	Oficio de respuesta a consulta de ciudadano Oficio de derivación de la denuncia - entidad competente Oficio de derivación de su denuncia - ciudadano Formato caso Memorando de derivación de la denuncia a la U.O Oficio de derivación de la denuncia al OCI Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad Oficio de denuncia desestimada - Ciudadano	Obtener la denuncia, datos de denunciante y evaluación.	35.2	Medio	No	Mitigar	Procedimiento para entrega de documentos reservados o confidenciales Incluir en los contratos acuerdos de confidencialidad con terceros encargados de la repartición de documentos.	3 meses 2 meses	DENUNCIAS	2	3	6	Aceptable
		Oficio de respuesta a consulta de ciudadano Oficio de derivación de la denuncia - entidad competente Oficio de derivación de su denuncia - ciudadano Formato caso Memorando de derivación de la denuncia a la U.O Oficio de derivación de la denuncia al OCI	Vende información de la denuncia, datos de denunciante y evaluación.			No	Mitigar	Implemetar en G. Denuncias la trasabilidad de acceso a información de denuncias Establecer sanciones económicas en los contratos con terceros.	6 meses 3 meses	DENUNCIAS / TIC				

N°	Riesgo	Activos de Información	Amenazas	Valor del riesgo en el negocio	Priorización	Tratamiento del Riesgo					Riesgo Residual			
						Control Existente	Opción de tratamiento	Detalle de control a realizar	Periodo	Responsable de implementar controles	Probabilidad de ocurrencia del riesgo	Impacto del riesgo en el negocio	Valor del riesgo en el negocio (I=e*h)	
		Oficio de solicitud de información sobre adopción de medidas correctivas - Entidad Oficio de denuncia desestimada - Ciudadano												
6	Emitir Oficio de respuesta con Pronunciamiento Incorrecto	Formato caso Registro de atención a ciudadano Información adicional requerida	No cumplir con los procedimientos establecidos	36	Medio	No	Mitigar	Implemetar en G. Denuncias la trasabilidad de acceso a información de denuncias	6 meses	DENUNCIAS	2	3	6	Aceptable
		Formato caso Registro de atención a ciudadano Información adicional requerida	Entrega información no verídica.			No	Mitigar	Establecer mecanismos de validación de documentos físicos.	3 meses	DENUNCIAS				
		Formato caso Registro de atención a ciudadano Información adicional requerida	Omite o no entrega información			No	Mitigar	Coordinar con la Gerencia del PAS la Operacionalizar el RIS	1 mes	DENUNCIAS				
7	Información procesada (denuncia en evaluación) es accedida por diferentes U.O sin control.	Aplicativo G. Denuncias Aplicativo SED Sist. Documentario SICGR - Trámite documentario	Accede a información de la denuncia en evaluación	24	Medio	No	Mitigar	> Implementar registro (log) de consultas realizadas por otras U.O > Actualizar los acuerdos de confidencialidad del personal con acceso a la información.	6 meses 1 mes	DENUNCIAS / TIC	1.4	2	2.8	Aceptable

ANEXO H

ANÁLISIS ECONÓMICO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Costo de Implementación

Riesgo 1	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo HH. (S/.)	Total
Obtener de la web CGR datos de denunciante y contenido de denuncia de la computadora usada por el denunciante.	Alto	> Implementar la eliminación de datos temporales de formulario web. > Limpiar formularios al cerrar sesión.	Programador.	2	320	S/. 35.00	S/. 22,400.00
			Documentador.	1	320	S/. 29.00	S/. 9,280.00
			Tester.	1	160	S/. 35.00	S/. 5,600.00
							S/. 37,280.00
		Total Riesgo 1					

Riesgo 2	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
Divulgar identidad de denunciante y contenido de denuncia desde el Sist. G. Denuncias o físico.	Alto	Revisión y bloqueo de usuarios que no han sido autorizados por DENUNCIAS	Administrador de BD	1	160	S/. 41.00	S/. 6,560.00
		Procedimiento para la atención de expedientes de denuncias a fin de restringir el acceso a personas no autorizadas.	Evaluadores	2	480	S/. 35.00	S/. 33,600.00
		Encriptar la información de los denunciantes en las Bases de Datos que lo contengan.	Administrador de BD	1	480	S/. 41.00	S/. 19,680.00
		Implemetar en Sist. G. Denuncias la trasabilidad de acceso a Información de denuncias.	Programador.	2	960	S/. 35.00	S/. 67,200.00
			Documentador.	1	160	S/. 29.00	S/. 4,640.00
			Administrador de BD	1	960	S/. 41.00	S/. 39,360.00
			Tester.	1	160	S/. 35.00	S/. 5,600.00
		Total Riesgo 2					**S/. 176,640.00**

Riesgo 3	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
No se puede atender oportunamente la denuncia recibida.	Medio	Actualizar antivirus y bloquear archivos con extensiones ejecutables.	Administrador de aplicaciones	1	80	S/. 41.00	S/. 3,280.00
		Establecer políticas de uso y configuración de equipos.	Evaluadores	2	120	S/. 35.00	S/. 8,400.00
		Comunicar al personal: > Las medidas de seguridad respecto a los tipos de equipos electricos a utilizar de acuerdo al nivel de voltios y amperios soportado por el circuito eléctrico. > Los horarios de mantenimiento y reparaciones fuera de horario de oficina.	Diseñador	1	8	S/. 29.00	S/. 232.00
		Establecer horarios de mantenimiento y reparaciones fuera de horario de oficina.	Operador de mantenimiento	1	8	S/. 29.00	S/. 232.00
		Total Riesgo 3					**S/. 12,144.00**

Riesgo 4	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
Perdida o extravío de documento de denuncia.	Medio	Establecer controles de seguimiento documental en los procedimientos de recepción, digitalización y derivación de documentos	Evaluadores	3	480	S/. 35.00	S/. 50,400.00
		Total Riesgo 4					**S/. 50,400.00**

Riesgo 5	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
Divulgar identidad de denunciante, contenido de denuncia y evaluación de documento de resolución durante el envío.	Medio	Procedimiento para entrega de documentos reservados o confidenciales	Evaluadores	2	480	S/. 35.00	S/. 33,600.00
		Incluir en los contratos acuerdos de confidencialidad con terceros encargados de la reparición de documentos.	Abogado	1	320	S/. 41.00	S/. 13,120.00
		Establecer sanciones económicas en los contratos con terceros.	Abogado	1	480	S/. 41.00	S/. 19,680.00
		Total Riesgo 5					**S/. 66,400.00**

Riesgo 6	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
Emitir Oficio de respuesta con Pronunciamiento Incorrecto	Medio	Implemetar en Sist. G. Denuncias la trasabilidad de acceso a Información de denuncias. (Cálculo en riesgo 2)	Programador/ Documentador/ tester/ Adm BD	4	960	S/. -	S/. -
		Establecer mecanismos de validación de documentos.	Evaluador	1	480	S/. 35.00	S/. 16,800.00
		Operacionalizar el RIS.	Coordinador de Denuncias	1	40	S/. 41.00	S/. 1,640.00
		Total Riesgo 6					**S/. 18,440.00**

Riesgo 7	Nivel	Control	Recursos	Cantidad	Tiempo (Horas)	Costo unitario	Total
Información procesada (denuncia en evaluación) es accedida por diferentes U.O sin control.	Medio	Implementar registro (log) de consultas realizadas por otras U.O	Administrador de BD	1	960	S/. 41.00	S/. 39,360.00
		Acuerdos de confidencialidad del personal con acceso a la Información.	Abogado	1	160	S/. 41.00	S/. 6,560.00
		Total Riesgo 7					**S/. 45,920.00**

Costo total de implementación de controles S/. 407,224.00

Impacto del Riesgo								
Riesgo	Impacto				económico	Costo por 1 denuncia	Cantidad de denunciantes	Costo por promedio mensual de denuncias
	Buena imagen y prestigio	Contractuales legales y regulatorios	Interrumpir las actividades u operaciones	Tiempo de recuperación de las operaciones				
Obtener de la web CGR datos de denunciante y contenido de denuncia de la computadora usada por el denunciante.	No determinado de nivel alto	5 a 50 UIT (S/. 19,750.00 a S/ 197,500.00) 25 UIT (S/. 9,8750.00)	2 personas para evaluar el sistema. (S/ 13,000.00)	80 horas	S/. 98,750.00 (Costo promedio de sanción grave de 25 UIT) S/ 13,000.00 (Horas hombre)	S/. 111,750.00	Total de denuncias desde el 2009 al 2015 es 15,239, el promedio mensual del 2012 al 2015 es **230 denuncias.**	S/. 22,725,500.00
Divulgar identidad de denunciante y contenido de denuncia desde el Sist: G. Denuncias o físico.	No determinado de nivel alto	5 a 50 UIT (S/. 19,750.00 a S/ 197,500.00) 25 UIT (S/. 9,8750.00)	3 personas para evaluar el sistema. (S/ 13,000.00)	80 horas	S/. 98,750.00 (Costo promedio de sanción grave de 25 UIT) S/ 13,000.00 (Horas hombre)	S/. 111,750.00		S/. 22,725,500.00
No se puede atender oportunamente la denuncia recibida.	No determinado de nivel medio	0.5 a 5 UIT (S/ 1,975 a 19,750) 3 UIT (S/. 11,850.00)	4 evaluadores de denuncias (S/ 23,000.00)	No determinado de nivel medio	S/. 11,850.00 (Costo promedio de sanción leve de 3 UIT) S/ 23,000.00 (Horas hombre)	S/. 34,850.00		S/. 2,748,500.00
Perdida o extravio de documento de denuncia.	No determinado de nivel medio	5 a 50 UIT (S/. 19,750.00 a S/ 197,500.00) 25 UIT (S/. 9,8750.00)	4 evaluadores de denuncias (S/ 23,000.00)	No determinado de nivel medio	S/. 11,850.00 (Costo promedio de sanción leve de 3 UIT) S/ 23,000.00 (Horas hombre)	S/. 34,850.00		S/. 22,735,500.00
Divulgar identidad de denunciante, contenido de denuncia y evaluación de documento de resolución durante el envío.	No determinado de nivel alto	5 a 50 UIT (S/. 19,750.00 a S/ 197,500.00) 25 UIT (S/. 9,8750.00)	No determinado de nivel bajo	No determinado de nivel bajo	S/. 98,750.00 (Costo promedio de sanción grave de 25 UIT)	S/. 98,750.00		S/. 22,712,500.00
Emitir Oficio de respuesta con Pronunciamiento incorrecto	No determinado de nivel medio	0.5 a 5 UIT (S/ 1,975 a 19,750) 3 UIT (S/. 11,850.00)	2 personas para evaluar el sistema. (S/ 11,000.00)	No determinado de nivel bajo	S/. 11,850.00 (Costo promedio de sanción leve de 3 UIT) S/ 11,000.00 (Horas hombre)	S/. 22,850.00		S/. 2,736,500.00
Información procesada (denuncia en evaluación) es accedida por diferentes U.O sin control.	No determinado de nivel bajo	0.5 a 5 UIT (S/ 1,975 a 19,750) 3 UIT (S/. 11,850.00)	No determinado de nivel bajo	No determinado de nivel bajo	S/. 11,850.00 (Costo promedio de sanción leve de 3 UIT)	S/. 11,850.00		S/. 2,725,500.00

El impacto legal ha sido calculado de las sanciones establecidas en la Ley de Protección de Datos Personales: Sanción Leve de 0.5 a 5 UIT, Sanción Grave de 5 a 50 UIT y Sanción Muy grave de 50 a 100 UIT.

Análisis Costo-Beneficio					
Costo de implementación de controles			Impacto del riesgo de no implemtar		Beneficio (Diferencia entre costo e impacto por riesgo)
Controles del Riesgo 1	S/.	37,280.00	Impacto económico del riesgo 1	S/. 22,725,500.00	S/. 22,688,220.00
Controles del Riesgo 2	S/.	176,640.00	Impacto económico del riesgo 2	S/. 22,725,500.00	S/. 22,548,860.00
Controles del Riesgo 3	S/.	12,144.00	Impacto económico del riesgo 3	S/. 2,748,500.00	S/. 2,736,356.00
Controles del Riesgo 4	S/.	50,400.00	Impacto económico del riesgo 4	S/. 22,735,500.00	S/. 22,685,100.00
Controles del Riesgo 5	S/.	66,400.00	Impacto económico del riesgo 5	S/. 22,712,500.00	S/. 22,646,100.00
Controles del Riesgo 6	S/.	18,440.00	Impacto económico del riesgo 6	S/. 2,736,500.00	S/. 2,718,060.00
Controles del Riesgo 7	S/.	45,920.00	Impacto económico del riesgo 7	S/. 2,725,500.00	S/. 2,679,580.00
	S/.	407,224.00			

Como se puede apreciar ante una posible sanción por incumplimiento legal e interrupciones el costo del impacto es mucho mayor que el costo de implementación de los controles.

Si comparamos el costo total de la implementación de los controles, este es aproximadamente el 15% del costo de la sanción de un riesgo de nivel medio como el caso del riesgo 6.